Centrify Zero Trust Privilege Services: Authentication Service, Privilege Elevation Service, and Audit and Monitoring Service

Centrify for ArcSight Integration Guide

July 2021

Centrify Corporation

Legal Notice

This document and the software described in this document are furnished under and are subject to the terms of a license agreement or a non-disclosure agreement. Except as expressly set forth in such license agreement or non-disclosure agreement, Centrify Corporation provides this document and the software described in this document “as is” without warranty of any kind, either express or implied, including, but not limited to, the implied warranties of merchantability or fitness for a particular purpose. Some states do not allow disclaimers of express or implied warranties in certain transactions; therefore, this statement may not apply to you.

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

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

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

Centrify, DirectControl, DirectAuthorize, DirectAudit, DirectSecure, DirectControl Express, Centrify for Mobile, Centrify for SaaS, DirectManage, Centrify Express, DirectManage Express, Centrify Suite, Centrify User Suite, Centrify Identity Service, Centrify Privilege Service and Centrify Server Suite are registered trademarks of Centrify Corporation in the United States and other countries. Microsoft, Active Directory, Windows, and Windows Server are either registered trademarks or trademarks of Microsoft Corporation in the United States and other countries.

Centrify software is protected by U.S. Patents 7,591,005; 8,024,360; 8,321,523; 9,015,103; 9,112,846; 9,197,670; 9,442,962 and 9,378,391.

The names of any other companies and products mentioned in this document may be the trademarks or registered trademarks of their respective owners. Unless otherwise noted, all of the names used as examples of companies, organizations, domain names, people and events herein are fictitious. No association with any real company, organization, domain name, person, or event is intended or should be inferred.

Contents

Introduction

This guide is written to assist Centrify customers with the task of easily integrating event data in ArcSight.

You can leverage the Centrify Add-on for ArcSight to normalize Centrify events in ArcSight so that you can view Centrify Authentication Service, Privilege Elevation Service, and Audit & Monitoring Service events when you use the ArcSight Console. For example, a sample event payload for an event named, Run as role failure, looks like this:

```
Apr 19 17:19:46 member.centrify.vms dzagent[1404]: WARN AUDIT_
TRAIL|Centrify Suite|DirectAuthorize - Windows|1.0|18|Run as role
failure|7|user=dwirth@centrify.vms userSid=S-1-5-21-3883016548-
1611565816-1967702834-1107 sessionId=3 centrifyEventID=6018
role=ROLE_SYSTEM_Archt/Global desktopguid=9766a262-c07b-4dbc-bad7-
8a48d1fa3983 command=C:\\Program Files\\Centrify\\DirectManage
Audit\\AuditManager\\Centrify DirectManage Audit Manager.msc
reason=The user name or password is incorrect desktopname=Default
networkroles=ROLE_SYSTEM_Archt/Global passwordprompted=True
```

This integration guide applies to the following ArcSight versions and Centrify Authentication Service, Privilege Elevation Service, and Audit & Monitoring Service releases:

ArcSight Versions	Centrify Authentication Service, Privilege Elevation Service, and Audit & Monitoring Service Releases
Enterprise Security Manager (ESM) 6.8.0	2016
ESM Console 6.8.0	2016.1
	2016.2
	2017
	2017.1
	2017.2
	2017.3

ArcSight Components

The following diagram illustrates the ArcSight components that interact with the Centrify Add-on for ArcSight:

Overview of the Integration Steps

The general integration steps that you perform are as follows:

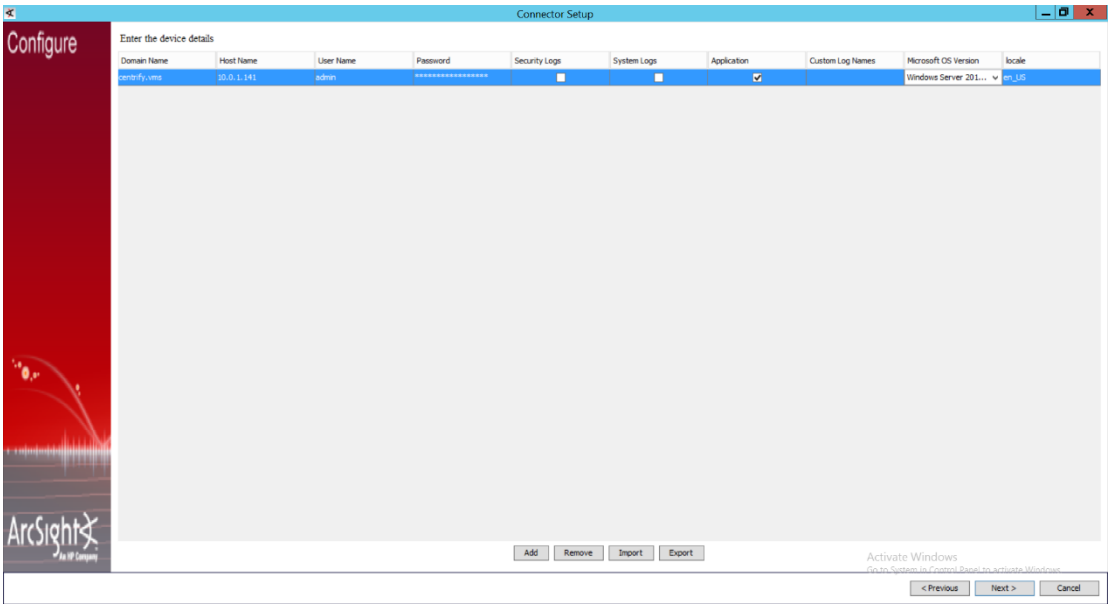
1. Collect Centrify event data from the Windows or Linux machine and forward it to the ArcSight ESM. You must install the ArcSight SmartConnector in the respective environment. (See ArcSight SmartConnector Installation.)
2. After successfully installing the ArcSight SmartConnector, place the properties file and the categorizer file in the appropriate location. (See Configuring FlexConnector for Data Normalization and Categorization.)
3. Open the ArcSight Console and the active channel that corresponds to the site connector. You should be able to view the real-time events being received in the active channel on the Windows or Linux machine. (See Verifying your configuration.)

ArcSight SmartConnector Installation

Follow the detailed steps in the ArcSight SmartConnector User Guide to install the ArcSight SmartConnector:

https://www.microfocus.com/documentation/arcsight/arcsight-smartconnectors/

IMPORTANT: As you install the ArcSight SmartConnector, make sure that you only select the Application check box to capture the Application logs.



Data Collection from a Windows Agent

Centrify software logs events in the Application logs on Windows machines. To capture the Application logs, Centrify uses the ArcSight SmartConnector for Windows.

There are a number of ways to collect data from Windows machines.
Some of the supported options include:

- Data collection from a stand-alone Windows machine:

Application logs are collected on a stand-alone Windows machine and parsed using the FlexConnector parser. Parsed events are forwarded to the ArcSight ESM where all of the data from Centrify Authentication Service, Privilege Elevation Service, and Audit & Monitoring Service is stored, and the ArcSight Console is used to access that data.

- Data collection using the Windows Event Forwarding (WEF) feature:

ArcSight SmartConnector supports WEF to collect Application logs forwarded by several Windows machines to a central machine. You install the ArcSight SmartConnector only on the central Windows machine that received the forwarded events and enable the WFE while installing the ArcSight SmartConnector.

- Data collection using the Active Directory (AD) Source:

ArcSight SmartConnector supports log collection for all of the member machines from the Active Directory Source itself. You install the ArcSight SmartConnector only on the AD server. During installation, you provide the Domain Controller name and its credentials. If the credentials and the domain name are correct, a list of all the member machines of that Domain Controller are seen in a new window. Users select only those Windows machines from which they want to collect Application logs.

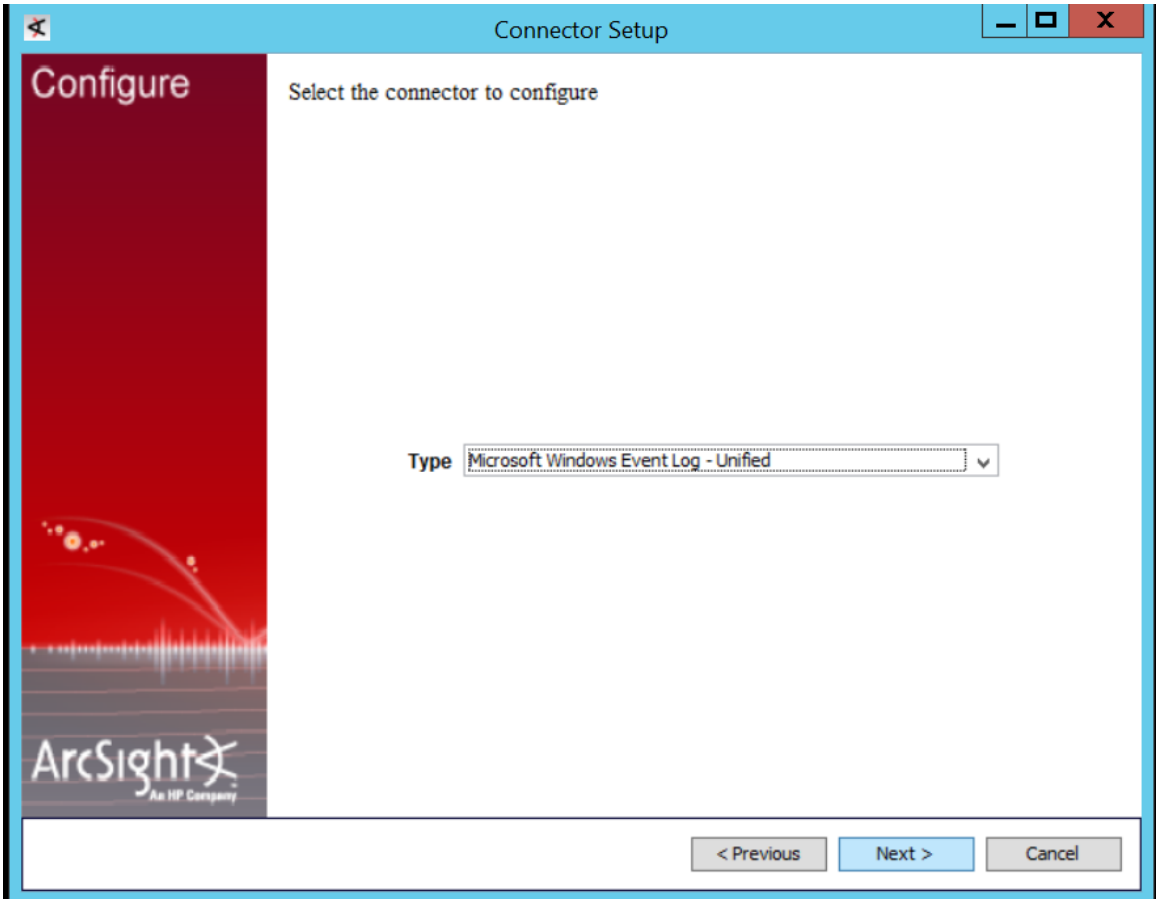
Installing the ArcSight SmartConnector on a Windows Agent

To install ArcSight SmartConnector on a Windows agent:

1. Execute the ArcSight SmartConnector binary for Windows.
2. Choose an installation folder.

   The default folder is:
   `C:\Programme Files\ArcSightSmartConnectors`

3. Wait for the installation to complete.



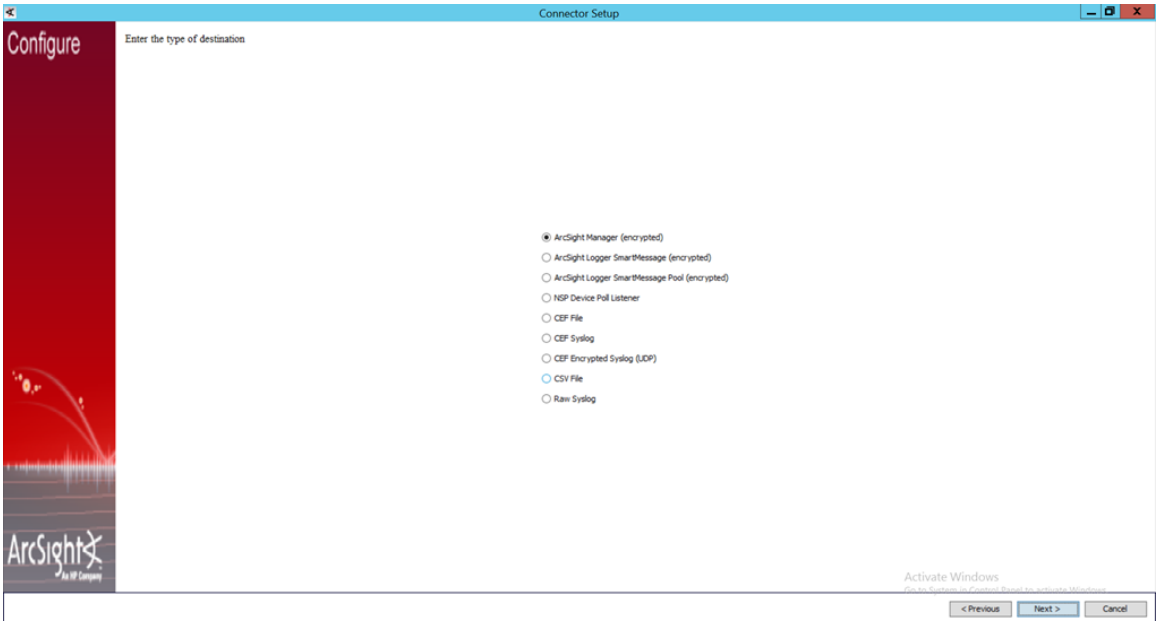
4. When you are prompted to select the connector to configure, select Microsoft Windows Event Log – Unified and click Next.
5. If you want to use Windows Event Forwarding, select Enable WEF.

   Note: You can also provide your Active Directory server parameters to get a list of all member VMs, and then select only those Windows machines from which you want to collect Application logs. As you are only installing on a stand-alone machine at this point, leave all of these parameters blank.

6. For the browser type, select **Enter Devices Manually** (do **not** use AD Source here).
7. Enter your host details.

   Make sure that you only select the Application check box to capture the Application logs because Centrify audit trail events **are only stored** in the

Windows Application logs.



8. When you are prompted for the type of destination, select ArcSight Manager (encrypted).

   You select ArcSight Manager (encrypted) because Centrify is forwarding the collected logs to the ArcSight ESM.

9. Provide your ArcSight ESM details:

   Enter the following information for the machine where the ArcSight ESM is installed:

   - Hostname
   - Port
   - Username
   - Password

10. Provide a name for your ArcSight SmartConnector.

    To assist you in assigning an applicable name, understand that the name is displayed on the ArcSight Console to identify those SmartConnector events that the console is receiving.

11. (Optional) If you want to use your ArcSight ESM certificate, select Import Certificate from your ArcSight ESM.

12. Specify whether you want to install the ArcSight SmartConnector as a service or as a stand-alone application.

    Install as a Service is generally preferred.

Data Collection from a Linux Agent

Centrify software logs events in the syslog directory on Linux machines. To collect the Linux syslog messages, choose from these options:

- Data collection from a stand-alone Linux machine:

To collect syslog messages from stand-alone Linux machines, use the Syslog File type of connector. You provide the directory location for syslog collection. Make sure that you have access to the syslog directory to avoid the error: permission denied.

- Data collection using the Syslog Daemon on a central Linux machine:

The Syslog Daemon type of connector is a syslogd-compatible daemon designed to work in operating systems that have no syslog daemon in their default configuration, such as Microsoft Windows.

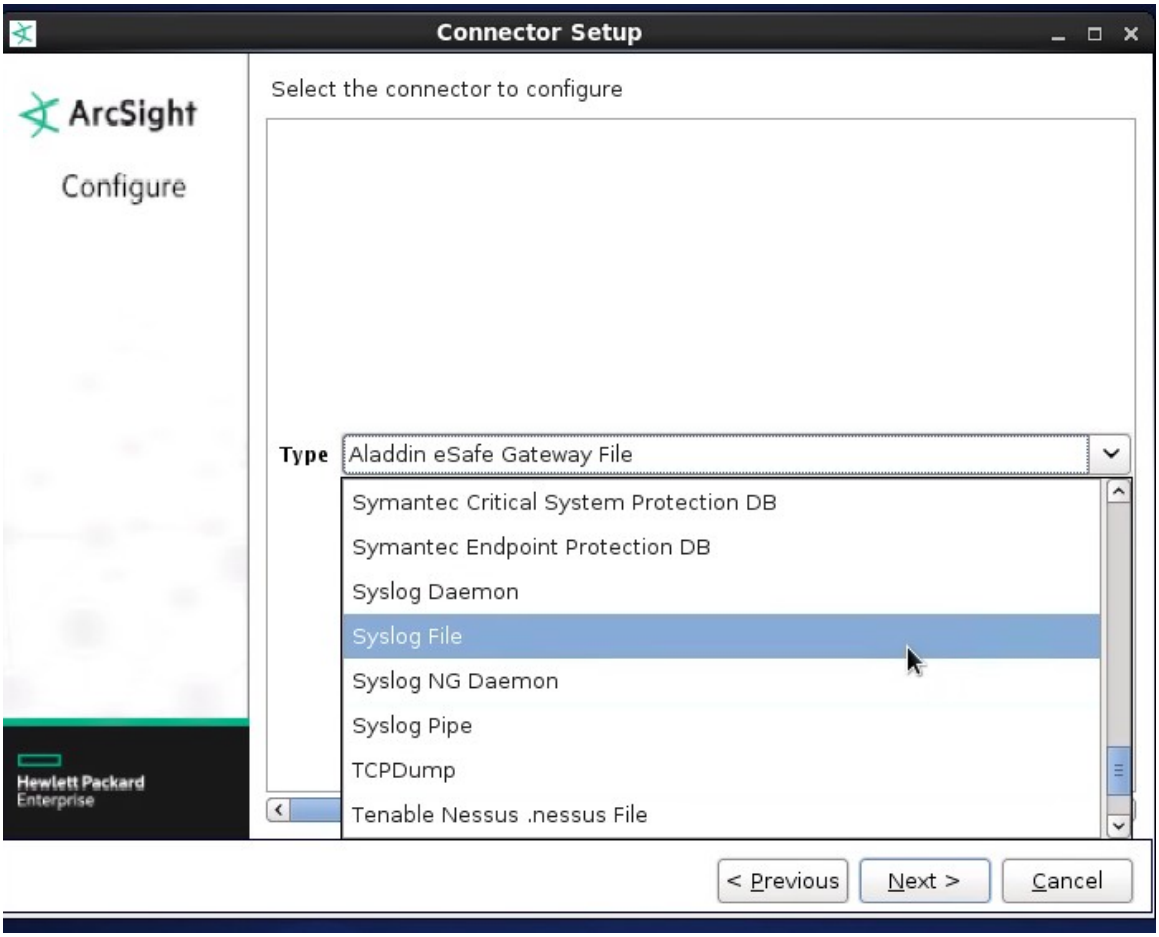
The SmartConnector for the Syslog Daemon implements a UDP receiver on port 514 (the default; which can also be configured) that can be used to receive syslog events. Use of the TCP protocol or a different port can be configured manually. You can forward the syslog from multiple Linux agents to a single machine. For example, when you configure the Syslog Daemon Connector on the 514 UDP port, you need to specify the receiving syslog port (514) and the protocol (UDP).

Installing the SmartConnector on a Linux Agent

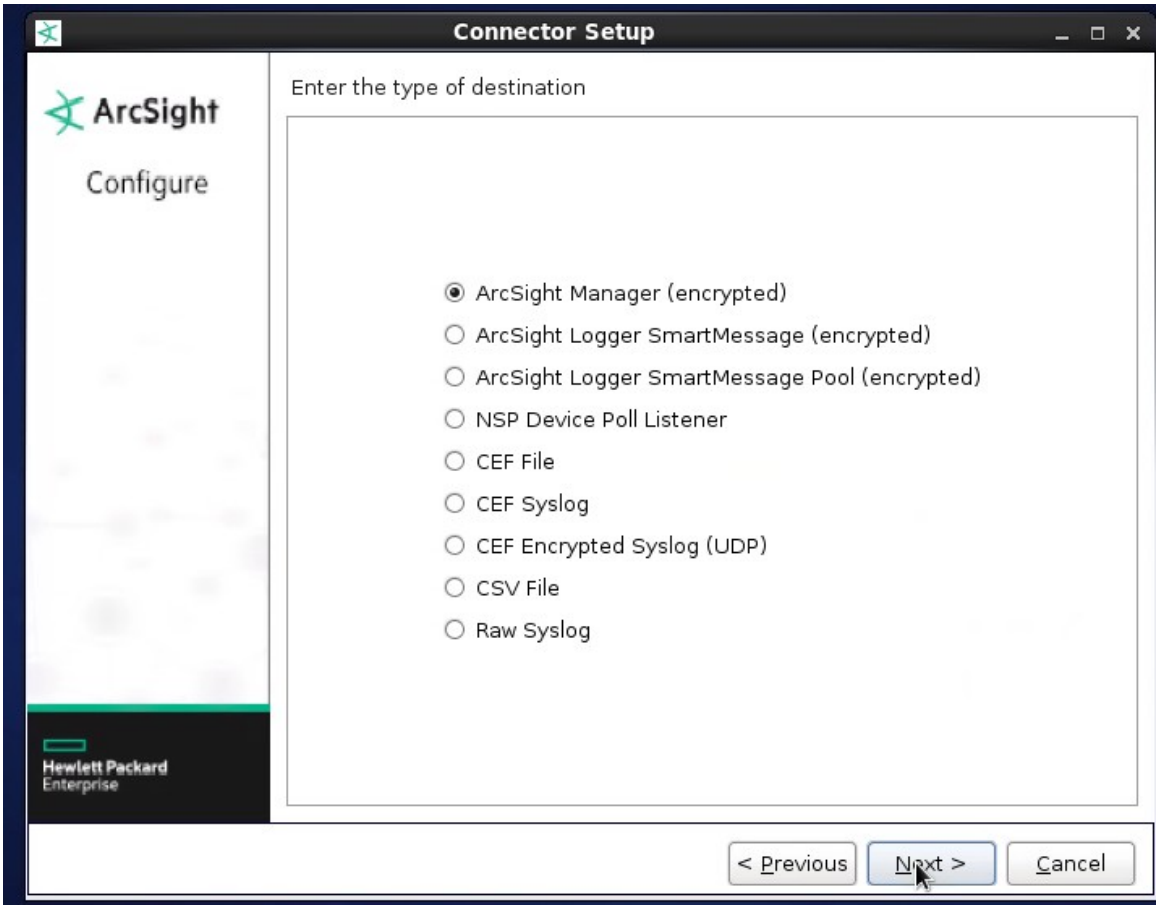
To install the SmartConnector:

1. Execute the SmartConnector binary for Linux.
2. Use the default name for the home folder.
3. Wait for the installation to complete.
4. When you are prompted to select the connector to configure, select **Syslog**

File.



5. Enter the file or directory of the syslog that you want to monitor.
6. When you are prompted to enter the type of destination, select **ArcSight Manager (encrypted) and click Next**.



You select ArcSight Manager (encrypted) because Centrify is forwarding the collected logs to the ArcSight ESM.

7. Provide your ArcSight ESM details.

   Enter the following information for the machine where the ArcSight ESM is installed:

   - Hostname
   - Port
   - Username
   - Password

8. Provide a name for your ArcSight connector.

   To assist you in assigning an applicable name, understand that the name is displayed on the ArcSight Console to identify those SmartConnector events that the console is receiving.

9. (Optional) If you want to use your ArcSight ESM certificate, select Import Certificate from your ArcSight ESM.

10. After the installation, check the status of the ArcSight SmartConnector service using following command:

    ```
    /etc/init.d/arc_syslog_file status
    ```

Configuring FlexConnector for Data Normalization and Categorization

When the ArcSight SmartConnector has been installed and configured to collect Centrify logs, the logs must be parsed and categorized using a customized Centrify FlexConnector. This FlexConnector contains two files for each Windows and Linux platform: a Parser and a Categorizer. You must place these files at specific locations depending on the operating system (OS) that you are using. Refer to the section below that applies to your OS.

Windows Application Logs

The two files needed for parsing and categorizing Windows application logs are in the folder:

`Centrify_windows_flexconnector`:

- The Categorizer file is: `centrify_suite.csv`
- The Parser file is: `application.centrify_audittrail_v2.sdkkeyvaluefilereader.properties`

To configure the Application logs for Windows:

1. Paste the Categorizer file, `centrify_suite.csv`, into the target location: `$ARCSIGHT_HOME\current\user\agent\acp\categorizer\current\centrify\`
2. Paste the Parser file: `application.centrify_audittrail_v2.sdkkeyvaluefilereader.properties` into the target location for your OS, as indicated by the following table:

Microsoft OS Version	Parser File Location
■ Windows Server 2008 R2 ■ Windows 7 SP1	$ARCSIGHT_HOME\user\agent\fcp\windowsfg\windows_2008
■ Windows Server 2012 ■ Windows Server 2012 R2 ■ Windows 8	$ARCSIGHT_HOME\user\agent\fcp\windowsfg\windows_2012
■ Windows Server 2016 ■ Windows 10	$ARCSIGHT_HOME\user\agent\fcp\windowsfg\windows_2016

3. Restart the SmartConnector service from the Windows Services.

Linux Syslogs

The two files needed for parsing and categorizing the Linux syslog are in the folder:

`Centrify_linux_flexconnector`

The two files are:

- Categorizer file: `centrify_suite.csv`
- Parser file:`centrify.subagent.sdkrfilereader.properties`

To configure syslogs for Linux:

1. Paste the Categorizer file, `centrify_suite.csv`, into the target location: `$ARCSIGHT_HOME/current/user/agent/acp/categorizer/current/Centrify/`
2. Paste the Parser file, `centrify.subagent.sdkrfilereader.properties`, into the target location, `$ARCSIGHT_HOME/user/agent/flexagent/syslog/`, regardless of the Linux version.
3. Restart the SmartConnector service from `/etc/init.d`

Verifying your configuration

After you finish configuring the FlexConnectors, Centrify recommends that you verify your configuration to make sure that events from Centrify are parsed correctly through the FlexConnectors.

To verify your configuration, generate some login events and then look for them either in the ESM Command Center or on the ESM Console.

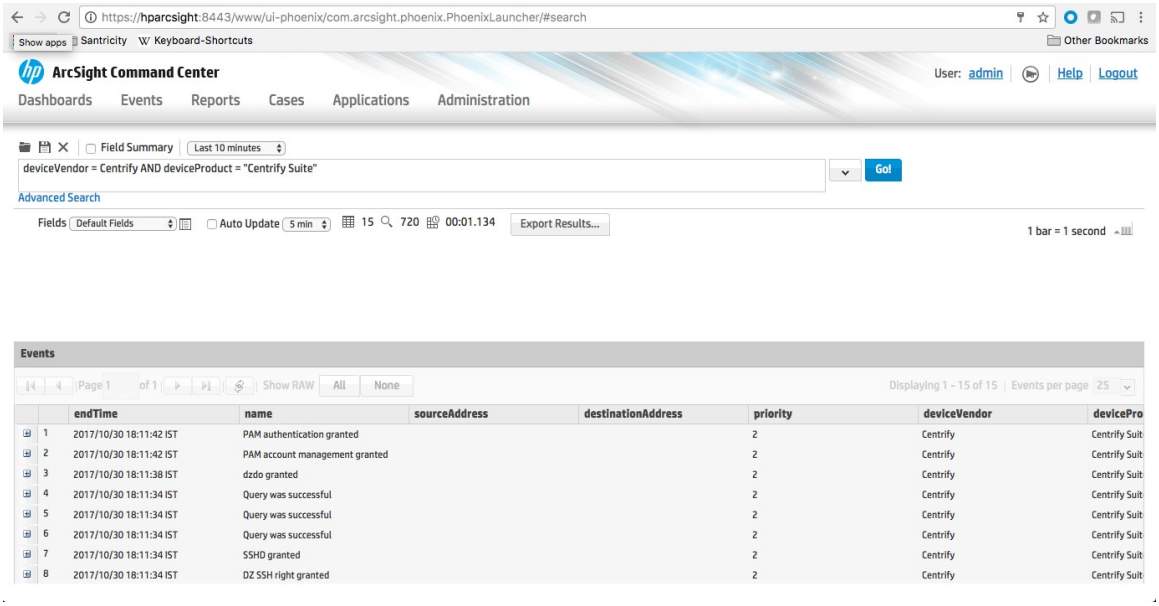
ESM Command Center

To look at login events using the ESM Command Center:

1. Generate login events.
2. Log in to the ESM Command Center.
3. Go to Events > Event Search.
4. Search for `deviceVendor="Centrify"` and `deviceProduct="Centrify Suite".`

   You should see all the authentication events as shown in the following

example:



ESM Console

To look at login events using the ESM Console:

1. Generate login events.
2. Log in to the ESM Console.
3. Go to Active Channels > Shared > All Active Channels > Centrify > Centrify Active Channels.

   You should see all of the Centrify audit events as shown in the following

example: