Hewlett Packard
Enterprise

HPE Security ArcSight User Behavior Analytics

Software Version: 5.0

Integration and Content Guide

July 21, 2016

Legal Notices

Warranty

The only warranties for Hewlett Packard Enterprise products and services are set forth in the express warranty statements accompanying such products and services. Nothing herein should be construed as constituting an additional warranty. Hewlett Packard Enterprise shall not be liable for technical or editorial errors or omissions contained herein.

The information contained herein is subject to change without notice.

The network information used in the examples in this document (including IP addresses and hostnames) is for illustration purposes only.

HPE Security ArcSight products are highly flexible and function as you configure them. The accessibility, integrity, and confidentiality of your data is your responsibility. Implement a comprehensive security strategy and follow good security practices.

This document is confidential.

Restricted Rights Legend

Confidential computer software. Valid license from Hewlett Packard Enterprise required for possession, use or copying. Consistent with FAR 12.211 and 12.212, Commercial Computer Software, Computer Software Documentation, and Technical Data for Commercial Items are licensed to the U.S. Government under vendor's standard commercial license.

Copyright Notice

Follow this link to see a complete statement of copyrights and acknowledgements:
https://www.protect724.hpe.com/docs/DOC-13026

Support

Contact Information

Phone	A list of phone numbers is available on the HPE Security ArcSight Technical Support Page: https://softwaresupport.hpe.com/documents/10180/14684/esp-support-contact-list
Support Web Site	https://softwaresupport.hpe.com
Protect 724 Community	https://www.protect724.hpe.com

Contents

Chapter 1: Overview

This guide provides information about integrating HPE Security ArcSight User Behavior Analytics (HPE ArcSight UBA) with ESM using Logger and ArcSight SmartConnectors to feed events to both applications. This guide also provides content information for HPE ArcSight UBA. For this release, Windows data sources are the only data sources supported. HPE ArcSight UBA integration with ESM requires the following:

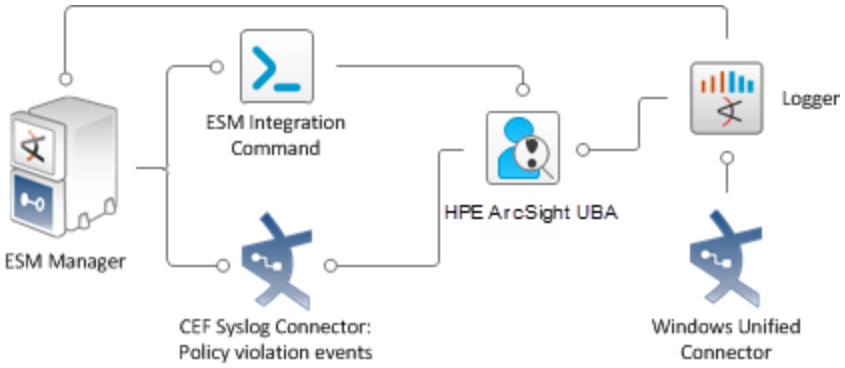
- Installing and configuring Logger and SmartConnectors to feed events to HPE ArcSight UBA and ESM
- Creating a security token in HPE ArcSight UBA
- Configuring an HPE ArcSight UBA Dashboard integration command in ESM
- Configuring a Logger forwarder to send events to HPE ArcSight UBA and ESM
- Creating and configuring Logger receivers to receive events from devices
- Configuring ArcSight SmartConnectors to collect events from devices and then forward the events to HPE ArcSight UBA and ESM

Architecture

HPE ArcSight UBA supports two architectures for integration with ESM and requires that HPE ArcSight UBA and ESM be installed on separate machines.

Logger Integration Architecture

The Logger integration architecture uses a Logger as the input device to ESM and HPE ArcSight UBA as shown in the following diagram:



The Logger integration architecture has the following components:

ArcSight Windows Unified Connector

The ArcSight Windows Unified Connector (WUC) receives events from devices and forwards the events to Logger. The above diagram represents a basic architecture. Your requirements might include multiple WUCs forwarding events to Logger.

Logger

Logger can send events to multiple destinations. For the HPE ArcSight UBA integration, Logger sends events to HPE ArcSight UBA and to ESM.

ESM

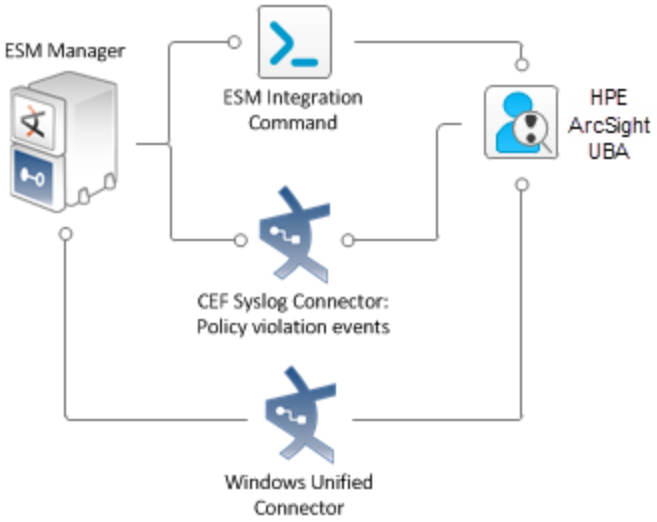
ESM receives events from Logger and HPE ArcSight UBA. ESM uses integration commands to create a secure connection with HPE ArcSight UBA. ESM also receives policy violation events from HPE ArcSight UBA.

HPE ArcSight UBA

HPE ArcSight UBA receives events from a Logger UDP forwarder. It analyzes the events and forwards all policy violation events to a CEF Syslog connector which forwards the events to ESM. ESM connects with HPE ArcSight UBA using the Dashboard Integration Command. The integration command opens a Web browser that requests the HPE ArcSight UBA web page using a secure token.

Connector Integration Architecture

The connector integration architecture uses a Windows Unified Connector to send events to ESM and HPE ArcSight UBA. A basic connector integration architecture has the following components:



The HPE ArcSight UBA connector integration architecture has the following components:

ArcSight Windows Unified Connector

An ArcSight Windows Unified Connector (WUC) receives events from devices and forwards the events to HPE ArcSight UBA and ESM. The above diagram represents a basic architecture. Your requirements might include multiple WUCs forwarding events to ESM and HPE ArcSight UBA.

HPE ArcSight UBA

HPE ArcSight UBA receives events from a WUC. It analyzes the events and forwards all policy violation events to a CEF Syslog connector which forwards the events to ESM. HPE ArcSight UBA connects with the ESM Console using the HPE ArcSight UBA Dashboard Integration Command. The integration command opens a Web browser that passes a token to HPE ArcSight UBA and the destination user name.

ESM

ESM receives events from a WUC. ESM uses the HPE ArcSight UBA Dashboard Integration Command to create a secure connection with HPE ArcSight UBA. ESM also receives policy violation events from HPE ArcSight UBA.

Chapter 2: Creating an HPE ArcSight User Behavior Analytics Token

To create a secure connection between HPE ArcSight UBA and ESM, a token is created in HPE ArcSight UBA and then copied and pasted within an ESM Integration Command. To create the token, perform the following procedure:

1. From the HPE ArcSight UBA Console, select **Configure** > **Connection Types** .
2. From the Connection Name list, select **CEFExport** then click the **Edit** button.
3. Enter the IP address or domain name for **Host** and select **Yes** for **Generate Token?**.
   The host is where the CEF Syslog connector is installed.
4. Click **Update**.

Note: The *ROLE_siemrole* can be granted more privileges from **Configure > Access Control > Manager Roles**, which gives the *siemuser* additional menu access.

Chapter 3: Downloading and Installing the User Behavior Analytics Arb File

To download the HPE ArcSight UBA content package from the Marketplace to the machine where you will run the ArcSight Console:

1. Log into the Marketplace (https://saas.hpe.com/marketplace/arcsight).
2. Navigate to **User Behavior Analytics** to find the HPE ArcSight UBA package, `HPE_ArcSight_User_Behavior_Analytics_1.1.arb` and download.

To install the content package on ESM:

1. Log into the ArcSight Console with an account that has administrative privileges.
2. In the Navigator panel, click the **Packages** tab.
3. Click **Import**  .
4. In the Open dialog, browse and select the package bundle file, and then select **Open**.
   The Progress tab of the Importing Packages dialog shows how the package bundle import is progressing. When the import is complete, the Results tab of the Importing Packages dialog is displayed together with the Packages for the Installation dialog.
5. In the Packages for Installation dialog, leave the /All Packages/ArcSight Solutions/HPE ArcSight User Behavior Analytics checkbox selected and click **Next**.
6. In the Installing Packages dialog, click **OK**.
7. In the Importing Packages dialog, click **OK**.
8. Navigate to ArcSight Solutions on the Packages tab of the Navigator panel, expand HPE ArcSight User Behavior Analytics to verify that the installation is successful and that the content is accessible.

Modifying the HPE ArcSight UBA Dashboard Integration Command

After you create the token in HPE ArcSight UBA, one of the ESM integration commands must be modified with the token key and the URL of the HPE ArcSight UBA application. In the following procedure, the HPE ArcSight UBA Dashboard command is used as an example of entering and saving the token key and URL of HPE ArcSight UBA server. You can also use the HPE ArcSight UBA User Information - Destination integration command or the HPE ArcSight UBA User Information - Source

integration command to accomplish the task. Perform the following procedure to modify the integration command:

1. Copy the token key (the key follows *token=*) from the token created in the HPE ArcSight UBA application.

   This step creates a user called "siemuser" and a role called "ROLE_siemrole" under **Configure > Access Control**. It also creates a token that can be used to access the Securonix application from ArcSight ESM. You can create a device URL in ArcSight ESM using following URL, https://<hostname>:<port>/Profiler/manageData/showUserSearch?token=f583dd40-4589-4f1b-82c9-7aef20729417&accountid=${destinationUserName}

   Note: Replace <hostname> with the appropriate network address/domain name and <port> with port number.

2. Log into the ArcSight Console.
3. Select the **Resources** tab and select **Integration Commands** from the drop-down list.
4. Navigate to ArcSight Solutions and expand it. Right-click **HPE ArcSight User Behavior Analytics > Integration Commands > HPE ArcSight UBA Dashboard . . .**.
5. Select HPE ArcSight UBA Dashboard for the command and HPE ArcSight UBA Server as the target. Click **OK**.
6. In the token Value field, paste the token key. In the HPuba Value field, enter the IP address or host name of the HPE ArcSight UBA server.
7. Click the **Save To Target** check box for both parameters. Once saved, you do not have enter either parameter again.
8. Click **OK**.

Chapter 4: Creating and Configuring Logger Receivers and Forwarder

Use the procedures in this chapter to create and configure Logger receivers. A receiver should be created and configured prior to installing and configuring a SmartConnector to send events to the receiver.

Creating a Logger Receiver

Perform the following procedure to create a Logger receiver:

1. Select the **Configuration** menu.
2. Click **Receivers**.
3. Click **Add**.
4. Enter a name for the receiver and select the type of receiver from the Type drop-down list.
5. Click **Next**.
6. Select the **Encoding** type from the drop-down list.
7. Select the **Source Type** from the drop-down list.
8. Click the **Enable** box to enable the receiver.
9. Click **Save**.

Configuring a Logger Receiver

Perform the following procedure to configure a Logger receiver:

1. Select the **Configuration** menu.
2. Click **Receivers**.
3. From the list of receivers, find the receiver you want to configure and click the receiver name.
4. Configure the receiver by selecting or entering values for the receiver's parameters.

Configuring a Logger Forwarder to Send CEF Events

Perform the following procedure to configure a forwarder to send CEF events to HPE ArcSight UBA:

1. Select **Configuration**.
2. Click **Forwarders**.
3. Click **Add**.

4. Enter values for the following parameters:
   - **Name** - the name of the forwarder
   - **Type** - select UDP Forwarder
   - **Filter Type** - select Unified Query
5. Click **Next**.
6. Enter or select values for the following fields:
   - **Query** - Enter the query (_deviceGroup in ["xx.xxx.xxx.xxx [SmartMessage Receiver]"]) and deviceProduct = "Microsoft Windows"
     For xx.xxx.xxx.xxx enter the IP address for the device sending Windows events.
   - **Filter by time range** - Click the box to filter by the time.
   - **Preserve Syslog Timestamp** - Select true to retain timestamps for the events sent.
   - **Preserve Original Syslog Sender** - Select true to retain information about the original device that sent the events.
   - **IP/Host** - Enter the IP address or host name for the machine where HPE ArcSight UBAruns.
   - **Port** - Enter the port where events should be sent to the machine where HPE ArcSight UBA runs.
7. Click **Save**.

Chapter 5: Using a SmartConnector to Send Events to Logger

Logger comes preconfigured with a SmartMessage Receiver. You can also create and configure new SmartMessage Receivers for multiple connector inputs to Logger. Configure the Logger receiver before configuring the connector so that the receiver name, port and output type are set prior to configuring the connector. See "Creating and Configuring Logger Receivers and Forwarder" on page 7 for more information. Use the following procedure to configure a SmartConnector to send events to Logger:

1. Install your SmartConnector using the SmartConnector Configuration Guide for your connector.
2. Specify Logger as the destination. Enter the Logger hostname or IP address and the name of the SmartMessage receiver.
   - To use the preconfigured receiver, use **SmartMessage Receiver** as the Receiver Name.
   - To use SmartMessage to communicate between your ArcSight SmartConnector and a Logger Appliance, configure the SmartConnector to use port 443.
   - To communicate between an ArcSight SmartConnector and Software Logger, configure the SmartConnector to use the port configured for the Software Logger.
   - For un-encrypted CEF syslog, enter the Logger hostname or IP address, the desired port, and choose UDP or TCP output.

Configuring a Connector to Send Syslog CEF Events

To configure a connector to send Syslog CEF events, perform the following procedure:

1. Run the AcrSight SmartConnector Installer.
2. Select **Add a Connector**. Click **Next**.
3. Select **Syslog Daemon**. Click **Next**.
4. Enter values for the following parameters:
   - **Network Port** - 514
   - **IP Address** - for the connector
   - **Protocol** - UDP
   - Forwarder - **False**
     Click **Next**.
5. Select **ArcSight Manager (encrypted)**. Click **Next**.
6. Enter a value for or select the following:

- **Manager Hostname** - Enter the IP address or host name of the ESM Manager.
- **Manager Port** - Enter the port number.
- **User** - Enter the user ID. This should be the user ID that was used to install the manager.
- **Password** -Enter the password for the user.
- Leave the default values for the remaining parameters.

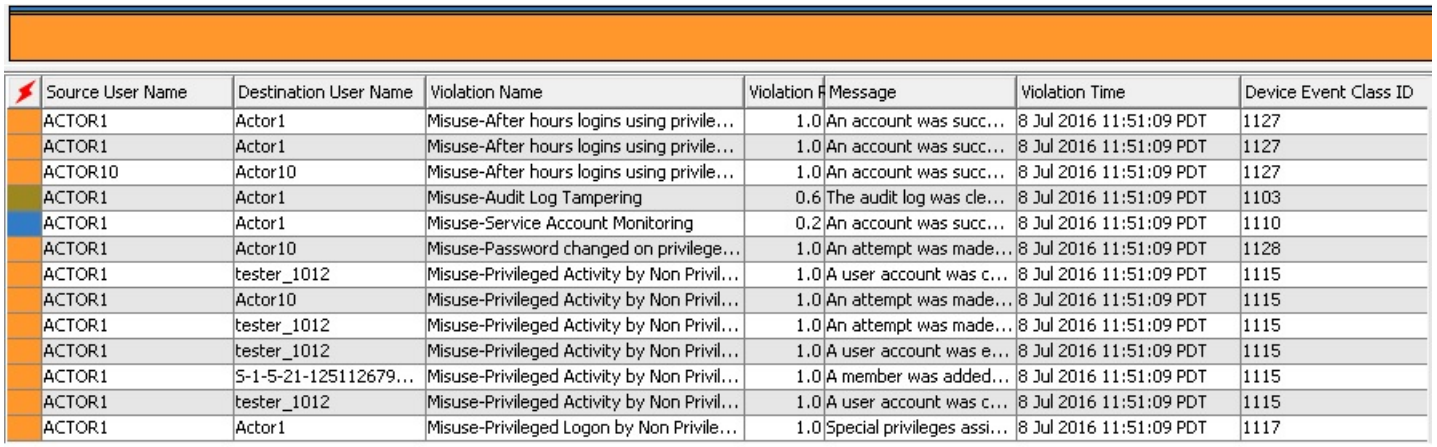
7. Click **Next**
8. Enter a name for the connector and any other information about the connector. Click **Next**. The certificate import window for the ArcSight Manager displays. Select Import the certificate to the connector from destination and click **Next**.
9. Complete the installation.

Chapter 6: Use Case Overview

HPE ArcSight UBA provides two use cases:

- **Privileged Account Access Violations Monitoring** - monitors access violations to privileged accounts
- **Privileged Account Action Violations Monitoring** - monitors unauthorized actions to privileged accounts

The integration between HPE ArcSight UBA and ESM is accomplished using integration commands. The integration commands are designed to work primarily with the active channels. For example, a partial view of the Privileged Account Violations Active Channel might have the following information:



Source User Name	Destination User Name	Violation Name	Violation R	Message	Violation Time	Device Event Class ID
ACTOR1	Actor1	Misuse-After hours logins using privile...	1.0	An account was succ...	8 Jul 2016 11:51:09 PDT	1127
ACTOR1	Actor1	Misuse-After hours logins using privile...	1.0	An account was succ...	8 Jul 2016 11:51:09 PDT	1127
ACTOR10	Actor10	Misuse-After hours logins using privile...	1.0	An account was succ...	8 Jul 2016 11:51:09 PDT	1127
ACTOR1	Actor1	Misuse-Audit Log Tampering	0.6	The audit log was cle...	8 Jul 2016 11:51:09 PDT	1103
ACTOR1	Actor1	Misuse-Service Account Monitoring	0.2	An account was succ...	8 Jul 2016 11:51:09 PDT	1110
ACTOR1	Actor10	Misuse-Password changed on privilege...	1.0	An attempt was made...	8 Jul 2016 11:51:09 PDT	1128
ACTOR1	tester_1012	Misuse-Privileged Activity by Non Privil...	1.0	A user account was c...	8 Jul 2016 11:51:09 PDT	1115
ACTOR1	Actor10	Misuse-Privileged Activity by Non Privil...	1.0	An attempt was made...	8 Jul 2016 11:51:09 PDT	1115
ACTOR1	tester_1012	Misuse-Privileged Activity by Non Privil...	1.0	An attempt was made...	8 Jul 2016 11:51:09 PDT	1115
ACTOR1	tester_1012	Misuse-Privileged Activity by Non Privil...	1.0	A user account was e...	8 Jul 2016 11:51:09 PDT	1115
ACTOR1	S-1-5-21-125112679...	Misuse-Privileged Activity by Non Privil...	1.0	A member was added...	8 Jul 2016 11:51:09 PDT	1115
ACTOR1	tester_1012	Misuse-Privileged Activity by Non Privil...	1.0	A user account was c...	8 Jul 2016 11:51:09 PDT	1115
ACTOR1	Actor1	Misuse-Privileged Logon by Non Privile...	1.0	Special privileges assi...	8 Jul 2016 11:51:09 PDT	1117

You can select an event, then right-click the event and select **Integration Commands > HPE ArcSight UBADashboards . . .** .

From the HPE ArcSight UBA Dashboard dialog, you can select from the following commands:

- **HPE ArcSight UBA Dashboard** - This command will display the HPE ArcSight UBA Dashboard dialog.
- **HPE ArcSight UBA User Information - Destination** - This command links you to information, in HPE ArcSight UBA, for the Destination User Name for the selected event.
- **HPE ArcSight UBA User Information - Source** - This command links you to information, in HPE ArcSight UBA, for the Source User Name for the selected event.

For the HPE ArcSight UBA Dashboard dialog above, click **OK** to display the Parameters dialog.

In the *sourceUserName*, enter the name of the user who violated the policy and click **OK** . You will be linked to the General Details page in HPE ArcSight UBA for the Source User Name. The General Details page provides information in the following categories:

- General Details
- Contact Details

- Workflow Details
- Employment History
- Custom Properties
- Change History

For further information about the Source User Name, you can select:

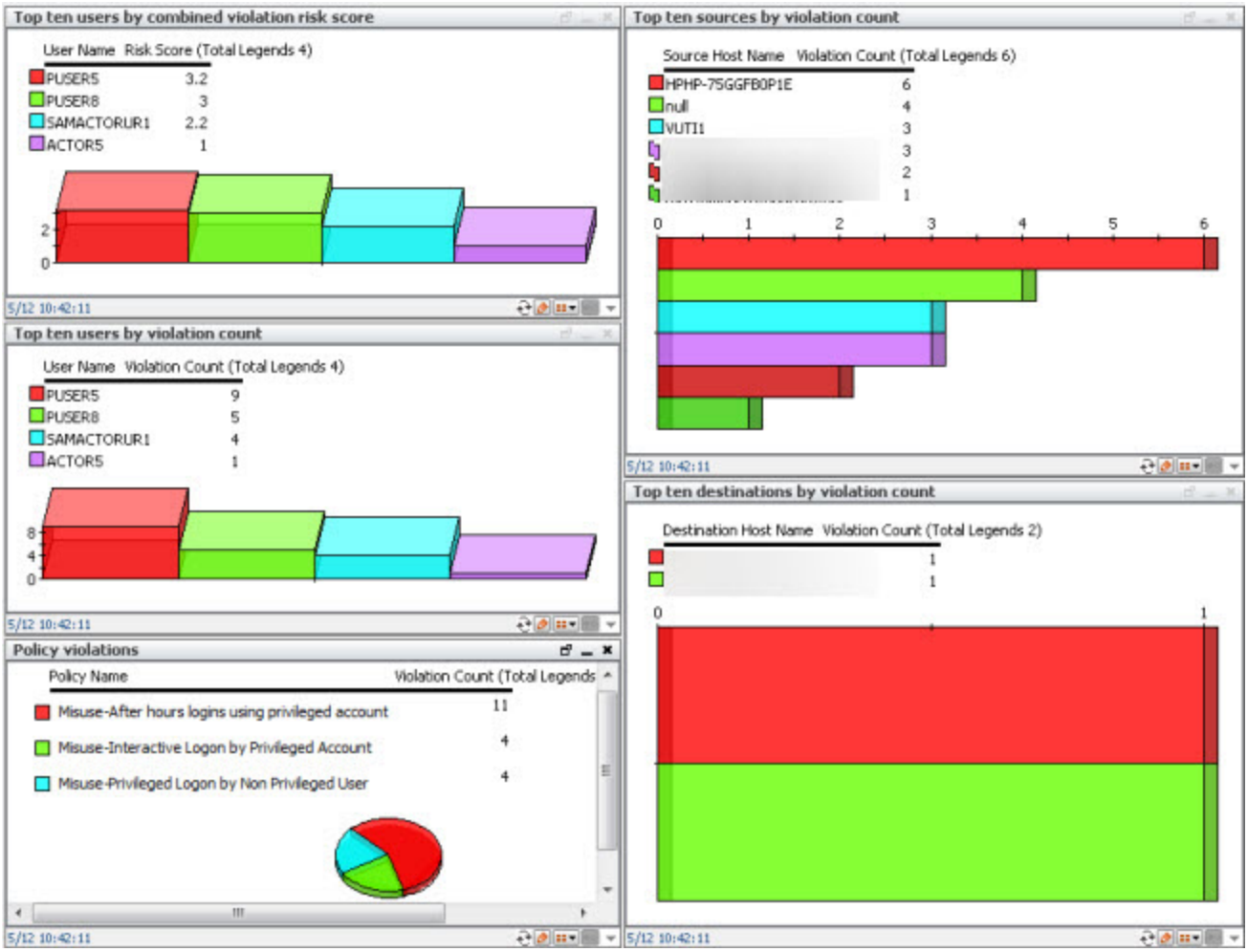
- Risk Scorecard
- Organization
- Peer Groups
- Monitor Access
- Monitor Activities
- Behavior Profile

The HPE ArcSight UBA User Information - Destination integration command is configured like the HPE ArcSight UBA User Information - Source Integration Command and provides similar information.

Privileged Account Access Violations Monitoring Use Case

The Privileged Account Access Violations Monitoring use case monitors login activities such as user logins, and violations of login policies.

The Privileged Account Access Violations Monitoring use case receives violations from HPE ArcSight UBA. This use case has one rule that is triggered when a violation is received from HPE ArcSight UBA. The use case has two dashboards: Privileged login violations and Privileged login violations overview. The Privileged login violations overview provides graphic views as shown in the following image:



You can click on a bar graph or pie chart and get drilldown detail information about:

- Source hostname
- Source IP address
- Source user name
- Policy name
- Violation risk score
- Violation time
- Violation count
- Destination host name
- Destination IP address
- Destination Zone

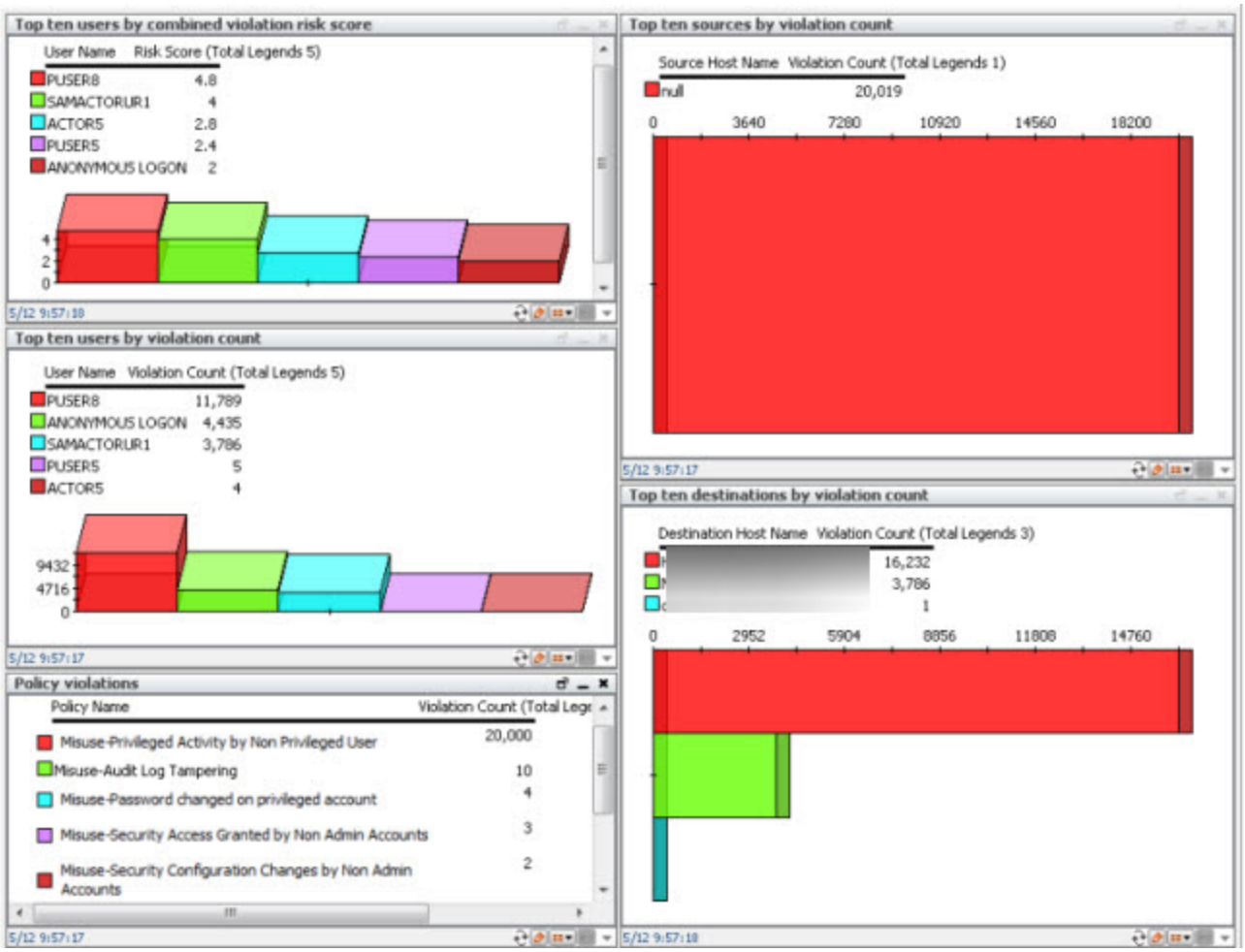
For information about all the resources for this use case, see User Behavior Analytics Resources By Type.

For the Privileged login violation overview dashboard, a drill-down for a specific user, source, destination will return information about all privileged account violations, including both the login and action violations for the user, source, destination and so forth. This ensures a complete view of user activity including user logins and actions after the login.

Privileged Account Action Violations Monitoring Use Case

The Privileged Account Action Violations Monitoring use case monitors action activities such as password changes, user account changes, log tampering actions, and other action policy violations.

The Privileged Account Action Violations Monitoring use case receives violations from HPE ArcSight UBA. This use case has one rule that is triggered when a violation is received from HPE ArcSight UBA. The use case has two dashboards: Privileged action violations and Privileged action violations overview. The Privileged action violations overview provides graphic views as shown in the following image:



You can click on a bar graph or pie chart and get drilldown detail information about:

- Source user name
- Policy name

- Message
- Violation risk score
- Violation time
- Violation count
- Destination hostname
- Destination IP address
- Destination Zone
- Employee first and last name, title, and employee ID

For information about all the resources for this use case, see User Behavior Analytics Resources By Type.

For the Privileged action violation overview dashboard, a drilldown for a specific user, source, destination will return information about all privileged account violations, including both the login and action violations for the user, source, destination and so forth. This ensures a complete view of user activity including user logins and actions after the login.

Appendix A: User Behavior Analytics Resources By Type

This appendix lists all the HPE ArcSight UBA resources by type.

Active Channels

Active Channels Resources

Resource	Description	URI
Privileged Account Violations	This active channel shows all privileged account violation events within the last 30 minutes.	`/All Active Channels/ArcSight Solutions/HPE ArcSight User Behavior Analytics/`

Active Lists

Active Lists Resources

Resource	Description	URI
Privileged Account Violations	This active list tracks privileged account violations including the violation details. The default expiration time for a active list is seven days, at which point the list entries expire. The active list is populated automatically by the Privileged Account.	`/All Active Lists/ArcSight Solutions/HPE ArcSight User Behavior Analytics/`

Dashboards

Dashboards Resources

Resource	Description	URI
Privileged login violations	This dashboard shows privileged login violation details sorted by the violation time (latest first).	`/All Dashboards/ArcSight Solutions/HPE ArcSight User Behavior Analytics/Privileged Account Login Violations/`
Privileged login violations overview	This dashboard shows an overview of privileged login violations in five panels: 1. Top ten users ranked by the user login violation combined risk score 2. Top ten users ranked by the user combined login violation count 3. Individual login policy violations with the count of each type of violation 4. Top ten sources ranked by the count of login violations originated from each source 5. Top ten destinations ranked by the count of login violations targeted at each destination	`/All Dashboards/ArcSight Solutions/HPE ArcSight User Behavior Analytics/Privileged Account Login Violations/`
Privileged action violations	This dashboard shows privileged action violations details sorted by the violation time (latest first).	`/All Dashboards/ArcSight Solutions/HPE ArcSight User Behavior Analytics/Privileged Action Violations/`
Privileged action violations overview	This dashboard shows an overview of privileged action violations in five panels: 1. Top ten users ranked by the user combined violation risk score 2. Top ten users ranked by the user combined violation count 3. Individual policy violations with the count of each violation 4. Top ten sources ranked by the count of violations originated from each source 5. Top ten destinations ranked by the count of violations targeted at each destination	`/All Dashboards/ArcSight Solutions/HPE ArcSight User Behavior Analytics/Privileged Action Violations/`

Field Sets

Field Sets Resources

Resource	Description	URI
Privileged Account Violations	This field set is used by the Privileged Account Violations active channel.	`/All Field Sets/ArcSight Solutions/HPE ArcSight User Behavior Analytics/`

Filters

Filters Resources

Resource	Description	URI
Privileged Account Violations	This filter identifies HPE ArcSight UBAprivileged account violation events.	/All Filters/ArcSight Solutions/HPE ArcSight User Behavior Analytics/

Integration Commands

Integration Commands Resources

Resource	Description	URI
HPE ArcSight UBA Dashboard	This integration command connects to the HPE ArcSight UBA Dashboard web page as the SIEMUser.	`/All Integration Commands/ArcSight Solutions/HPE ArcSight User Behavior Analytics/`
HPE ArcSight UBA User Information - Destination	After you right-click an event in the active channel, this integration command connects to the HPE ArcSight UBA web page displaying details for the user populated in the Destination User Name field of the event.	`/All Integration Commands/ArcSight Solutions/HPE ArcSight User Behavior Analytics/`
HPE ArcSight UBA User Information - Source	After you right-click an event in the active channel, this integration command connects to the HPE ArcSight UBA web page displaying details for the user populated in the Source User Name field of the event.	`/All Integration Commands/ArcSight Solutions/HPE ArcSight User Behavior Analytics/`

Integration Configurations

Integration Configurations Resources

Resource	Description	URI
HPE ArcSight UBADashboard	This integration configuration binds the HPE ArcSight UBA integration commands to the HPE ArcSight UBA Server target.	`/All Integration Configurations/ArcSight Solutions/HPE ArcSight User Behavior Analytics/`

Integration Targets

Integration Targets Resources

Resource	Description	URI
HPE ArcSight UBA Server	This integration target stores the URL parameters for the integration commands: hostname or IP address of the HPE ArcSight UBA, and the security. The integration target can be used to supply parameter values to the HPE ArcSight UBA integration commands.	`/All Integration Targets/ArcSight Solutions/HPE ArcSight User Behavior Analytics/`

Queries

Queries Resources

Resource	Description	URI
After-hours Logins Using a Privileged Account	This query selects information about after-hours logins using a privileged account.	`/All Queries/ArcSight Solutions/HPE ArcSight User Behavior Analytics/Privileged Account Login Violations/`
Policy violations	This query selects information about the privileged account login policy violations along with the number of times each type of violation occurred.	`/All Queries/ArcSight Solutions/HPE ArcSight User Behavior Analytics/Privileged Account Login Violations/`
Privileged Logins by Unauthorized User	This query selects information about the privileged account logins by unauthorized user. This happens when a user account with privileged access is detected during logon and that user account is not in the approved high-privileged list maintained by HP ArcSight UBA.	`/All Queries/ArcSight Solutions/HPE ArcSight User Behavior Analytics/Privileged Account Login Violations/`

Queries Resources, continued

Resource	Description	URI
Service Account Interactive Logins	This query selects information about successful interactive logins by accounts tagged as service accounts.	/All Queries/ArcSight Solutions/HPE ArcSight User Behavior Analytics/Privileged Account Login Violations/
Top ten users by violation count	This query selects information about top ten users sorted by the combined action violation count.	/All Queries/ArcSight Solutions/HPE ArcSight User Behavior Analytics/Privileged Account Login Violations/
Top ten destinations by violation count	This query selects information about the top ten destinations sorted by the count of login violations targeted to the destination.	/All Queries/ArcSight Solutions/HPE ArcSight User Behavior Analytics/Privileged Account Login Violations/
Top ten sources by violation count	This query selects information about the top ten sources sorted by the count of login violations originated from the source.	/All Queries/ArcSight Solutions/HPE Arcsight User Behavior Analytics/Privileged Account Login Violations/
Top ten user logins by consolidated violations risk score	This query selects information about the top ten users ranked by the user login violations combined risk score.	/All Queries/ArcSight Solutions/HPE ArcSight User Behavior Analytics/Privileged Account Login Violations/
Audit Log Tampering	This query selects information about audit log tampering activity.	/All Queries/ArcSight Solutions/HPE ArcSight User Behavior Analytics/Privileged Action Violations/
Password Changes on a Privileged Account	This query selects information about the password changes for accounts in the approved high-privileged accounts list maintained by HP ArcSight UBA.	/All Queries/ArcSight Solutions/HPE ArcSight User Behavior Analytics/Privileged Action Violations/
Policy violations	This query selects information about privileged action policy violations along with the number of times each violation occurred.	/All Queries/ArcSight Solutions/HPE ArcSight User Behavior Analytics/Privileged Action Violations/

Queries Resources, continued

Resource	Description	URI
Privileged Activities by Unauthorized User	This query selects information about the privileged activity by unauthorized users. This happens when privileged activity is detected by users who are not in the approved high-privileged accounts list maintained by HP ArcSight UBA.	/All Queries/ArcSight Solutions/HPE ArcSight User Behavior Analytics/Privileged Action Violations/
Security Access Granted by Unauthorized Account	This query selects information about the violation activity when a user is granted security access by a user who is not in the approved high-privileged accounts list maintained by HP ArcSight UBA.	/All Queries/ArcSight Solutions/HPE ArcSight User Behavior Analytics/Privileged Action Violations/
Security Configuration Changes Made by Unauthorized Account	This query selects information about violation activity when security configuration changes are made by an unauthorized account.	/All Queries/ArcSight Solutions/HPE ArcSight User Behavior Analytics/Privileged Action Violations/
Top ten destinations by violation count	This query selects information about the top ten destinations sorted by the count of action violations targeted to the destination.	/All Queries/ArcSight Solutions/HPE ArcSight User Behavior Analytics/Privileged Action Violations/
Top ten sources by violation count	This query selects information about the top ten sources sorted by the count of action violations originated from the source.	/All Queries/ArcSight Solutions/HPE ArcSight User Behavior Analytics/Privileged Action Violations/
Top ten users by combined violation risk score	This query selects information about the top ten users sorted by the user action violation combined risk score.	/All Queries/ArcSight Solutions/HPE ArcSight User Behavior Analytics/Privileged Action Violations/
Top ten users by violation count	This query selects information about the top ten users sorted by the combined action violation count.	/All Queries/ArcSight Solutions/HPE ArcSight User Behavior Analytics/Privileged Action Violations/
User Activity Details	This query selects information about the policy violation details. It is used in drilldowns for the privileged user activity dashboards.	/All Queries/ArcSight Solutions/HPE ArcSight User Behavior Analytics/

Query Viewers

Query Viewers Resources

Resource	Description	URI
After-hours Logins Using a Privileged Account	This query viewer shows after-hours logins using a privileged account.	/All Query Viewers/ArcSight Solutions/HPE ArcSight User Behavior Analytics/Privileged Account Login Violations/
Policy violations	This query viewer shows the privileged account login policy violations along with the number of times each violation occurred.	/All Query Viewers/ArcSight Solutions/HPE ArcSight User Behavior Analytics/Privileged Account Login Violations/
Privileged Logins by Unauthorized User	This query viewer shows the privileged account logins by unauthorized users.	/All Query Viewers/ArcSight Solutions/HPE ArcSight User Behavior Analytics/Privileged Account Login Violations/
Service Account Interactive Logins	This query viewer shows interactive successful logins by accounts tagged as service accounts.	/All Query Viewers/ArcSight Solutions/HPE ArcSight User Behavior Analytics/Privileged Account Login Violations/
Top ten destinations by violation count	This query viewer shows the top ten destinations sorted by the count of login violations targeted to the destination.	/All Query Viewers/ArcSight Solutions/HPE ArcSight User Behavior Analytics/Privileged Account Login Violations/
Top ten destinations by violation count	This query viewer shows the top ten destinations sorted by the count of action violations targeted to the destination.	/All Query Viewers/ArcSight Solutions/HPE ArcSight User Behavior Analytics/Privileged Account Action Violations/
Top ten sources by violation count	This query viewer shows the top ten sources sorted by the count of login violations originated from the source.	/All Query Viewers/ArcSight Solutions/HPE ArcSight User Behavior Analytics/Privileged Account Login Violations/
Top ten sources by violation count	This query viewer shows the top ten sources sorted by the count of action violations originated from the source.	/All Query Viewers/ArcSight Solutions/HPE ArcSight User Behavior Analytics/Privileged Account Action Violations/
Top ten users by combined violation risk score	This query viewer shows the top ten users sorted by the user login violation combined risk score.	/All Query Viewers/ArcSight Solutions/HPE ArcSight User Behavior Analytics/Privileged Account Login Violations/

Query Viewers Resources, continued

Resource	Description	URI
Top ten users by combined violation risk score	This query viewer shows the top ten users sorted by the user action violation combined risk score.	/All Query Viewers/ArcSight Solutions/HPE ArcSight User Behavior Analytics/Privileged Account Action Violations/
Top ten users by violation count	This query viewer shows the top ten users sorted by the combined login violation count.	/All Query Viewers/ArcSight Solutions/HPE ArcSight User Behavior Analytics/Privileged Login Violations/
Top ten users by violation count	This query viewer shows the top ten users sorted by the combined action violation count.	/All Query Viewers/ArcSight Solutions/HPE ArcSight User Behavior Analytics/Privileged Action Violations/
Audit Log Tampering	This query viewer shows audit log tampering activity.	/All Query Viewers/ArcSight Solutions/HPE ArcSight User Behavior Analytics/Privileged Action Violations/
Password Changes on a Privileged Account	This query viewer shows the password changes for accounts in the privileged accounts list maintained by HPE ArcSight UBA.	/All Query Viewers/ArcSight Solutions/HPE ArcSight User Behavior Analytics/Privileged Action Violations/
Policy violations	This query viewer shows privileged action policy violations along with the number of times each type of violation occurred.	/All Query Viewers/ArcSight Solutions/HPE ArcSight User Behavior Analytics/Privileged Action Violations/
Privileged Activities by Unauthorized User	This query viewer shows the privileged activity by unauthorized users. This happens when privileged activity is detected by users who are not in the approved high-privileged accounts list maintained by the HP UBA.	/All Query Viewers/ArcSight Solutions/HPE ArcSight User Behavior Analytics/Privileged Action Violations/
Security Access Granted by Unauthorized Account	This query viewer shows the violation activity when a user is granted security access by a user who is not in the approved high-privileged accounts list maintained by the HP UBA.	/All Query Viewers/ArcSight Solutions/HPE ArcSight User Behavior Analytics/Privileged Action Violations/
Security Configuration Changes Made by Unauthorized Account	This query viewer shows the violation activity when security configuration changes are made by a user who is not in the approved high-privileged accounts list maintained by the HP UBA.	/All Query Viewers/ArcSight Solutions/HPE ArcSight User Behavior Analytics/Privileged Action Violations/
User Activity Details	This query displays the details about the policy violations. It is used in drilldowns for the privileged user activity dashboards.	/All Query Viewers/ArcSight Solutions/HPE ArcSight User Behavior Analytics/

Rules

Rules Resources

Resource	Description	URI
Privileged Account Violations	This rule triggers when a privileged account violation is reported by the HPE ArcSight UBA. The rule then creates a new entry in the Privileged Account Violations active list.	`/All Rules/ArcSight Solutions/HPE ArcSight User Behavior Analytics/`

Use Cases

Use Cases Resources

Resource	Description	URI
Privileged Account Access Violations Monitoring	This use case tracks privileged account access (login) violations providing statistical information about the violations.	`/All Use Cases/ArcSight Solutions/HPE ArcSight User Behavior Analytics/`
Privileged Account Action Violations Monitoring	This use case tracks privileged account action violations providing statistical information about the violations.	`/All Use Cases/ArcSight Solutions/HPE ArcSight User Behavior Analytics/`

Send Documentation Feedback

If you have comments about this document, you can contact the documentation team by email. If an email client is configured on this system, click the link above and an email window opens with the following information in the subject line:

Feedback on Integration and Content Guide (User Behavior Analytics 5.0)

Just add your feedback to the email and click send.

If no email client is available, copy the information above to a new message in a web mail client, and send your feedback to arc-doc@hpe.com.

We appreciate your feedback!