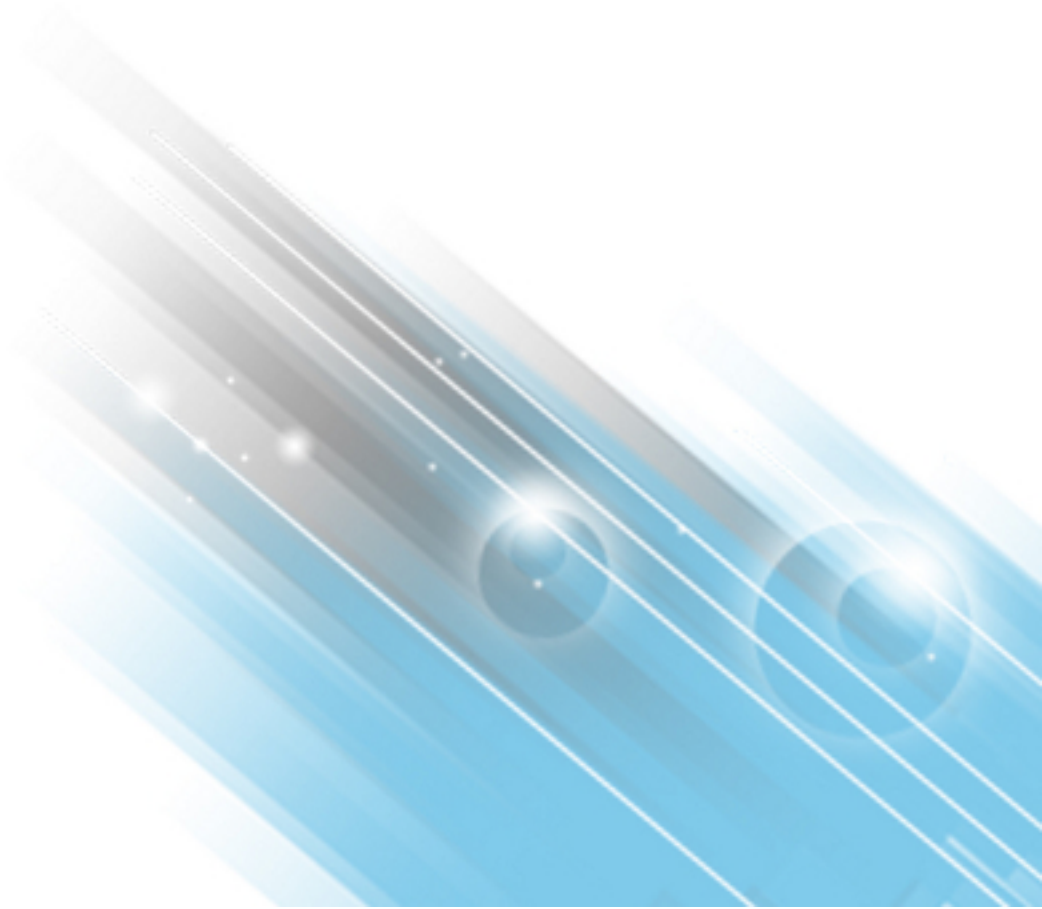
HP ArcSight User Behavior Analytics

Software Version: 1.0

HP User Behavior Analytics Integration and Content Guide



May 29, 2015

Legal Notices

Warranty

The only warranties for HP 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. HP 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.

HP 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 HP 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:
http://www.hpenterprisesecurity.com/copyright

Support

Contact Information

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

Contents

Chapter 1: Overview

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

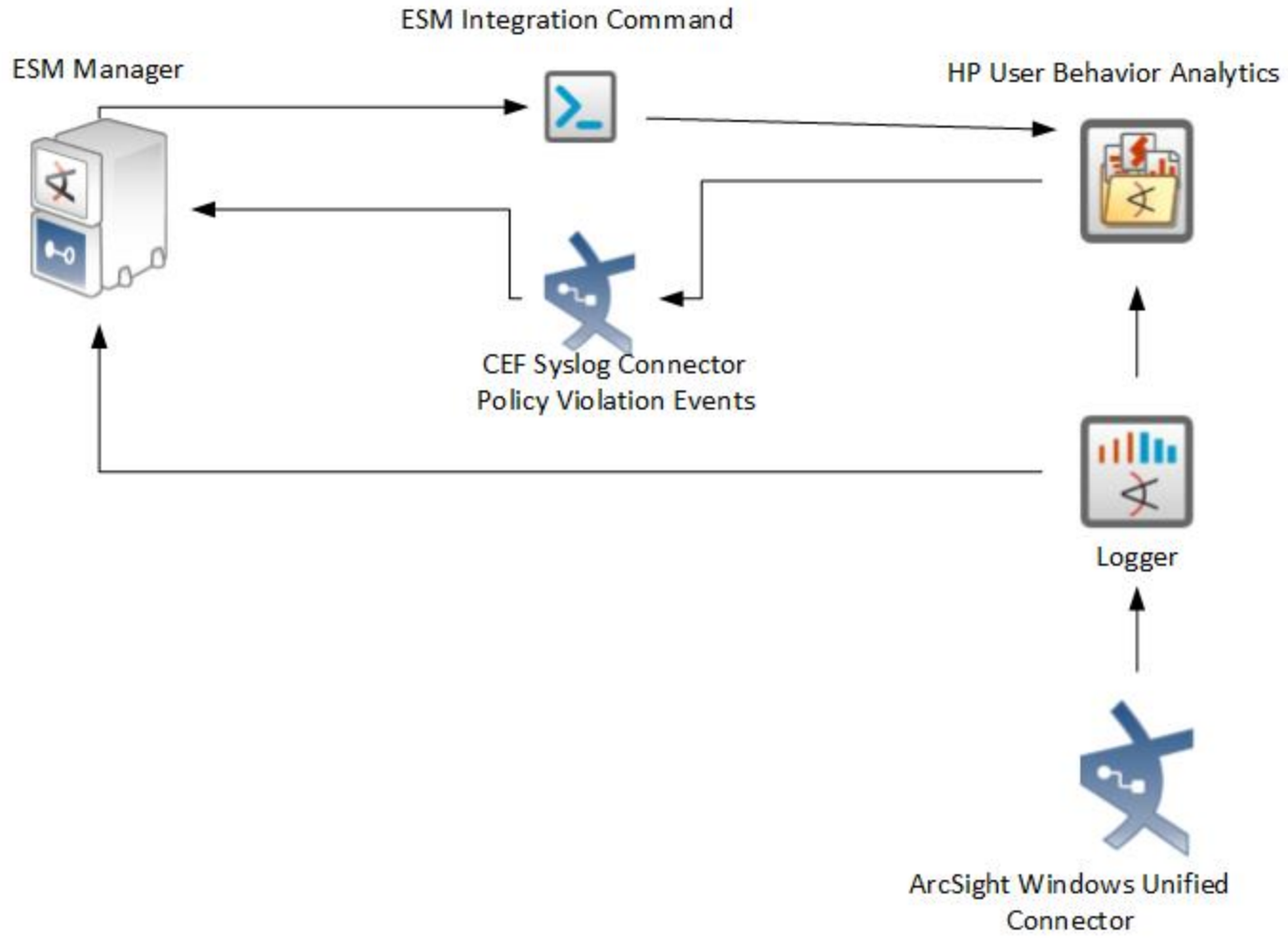
- Installing and configuring Logger and SmartConnectors to feed events to HP UBA and ESM
- Creating a security token in HP UBA
- Configuring an HP UBA Dashboard integration command in ESM
- Configuring a Logger forwarder to send events to HP UBA and ESM
- Creating and configuring Logger receivers to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

Architecture

HP User Behavior Analytics (HP UBA) supports two architectures for integration with ESM and requires that HP 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 HP User Behavior Analytics 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 HP User Behavior Analytics (HP UBA) integration, Logger sends events to HP UBA and to ESM.

ESM

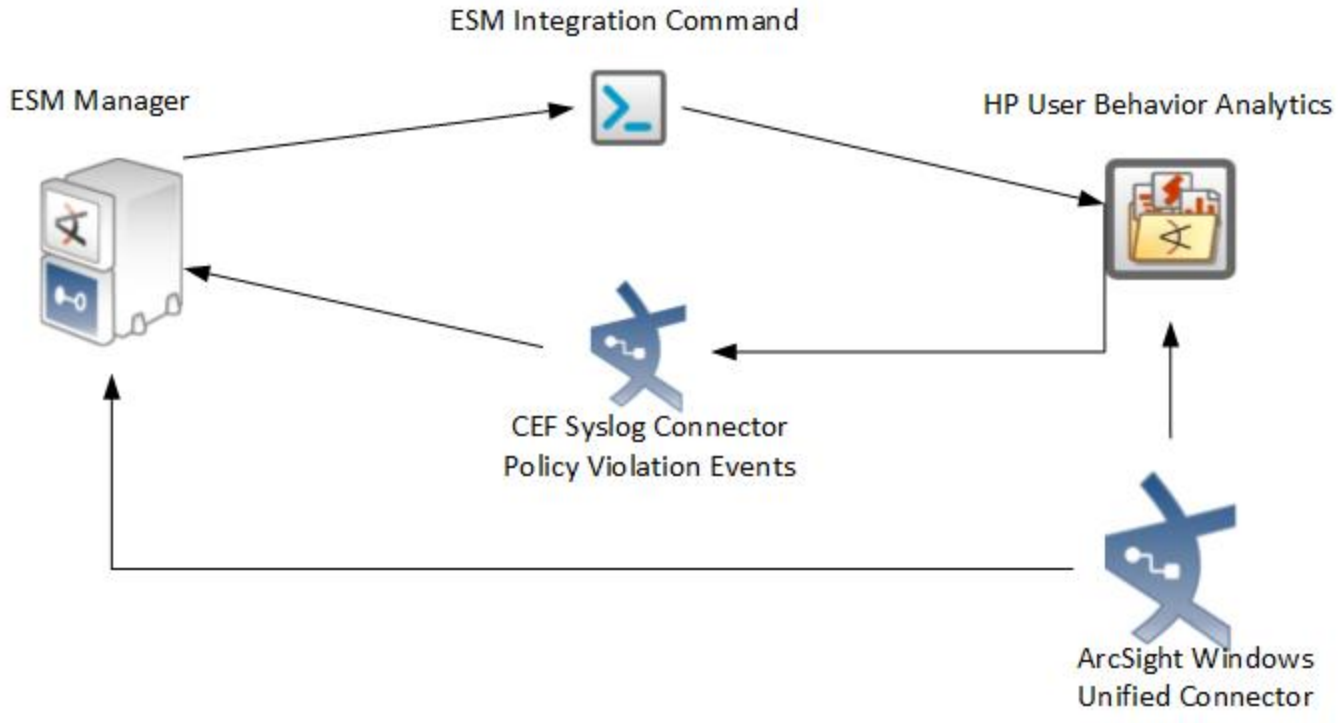
ESM receives events from Logger and HP UBA. ESM uses integration commands to create a secure connection with HP UBA. ESM also receives policy violation events from HP UBA.

HP User Behavior Analytics

HP 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 HP UBA using the HP UBA Dashboard Integration Command. The integration command opens a Web browser that requests the HP 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 HP User Behavior Analytics. A basic connector integration architecture has the following components:



The HP User Behavior Analytics 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 HP User Behavior Analytics and ESM. The above diagram represents a basic architecture. Your requirements might include multiple WUCs forwarding events to ESM and HP UBA.

HP User Behavior Analytics

HP User Behavior Analytics 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. HP UBA connects with the ESM Console using the HP UBA Dashboard Integration Command. The integration command opens a Web browser that passes a token to HP UBA and the destination user name.

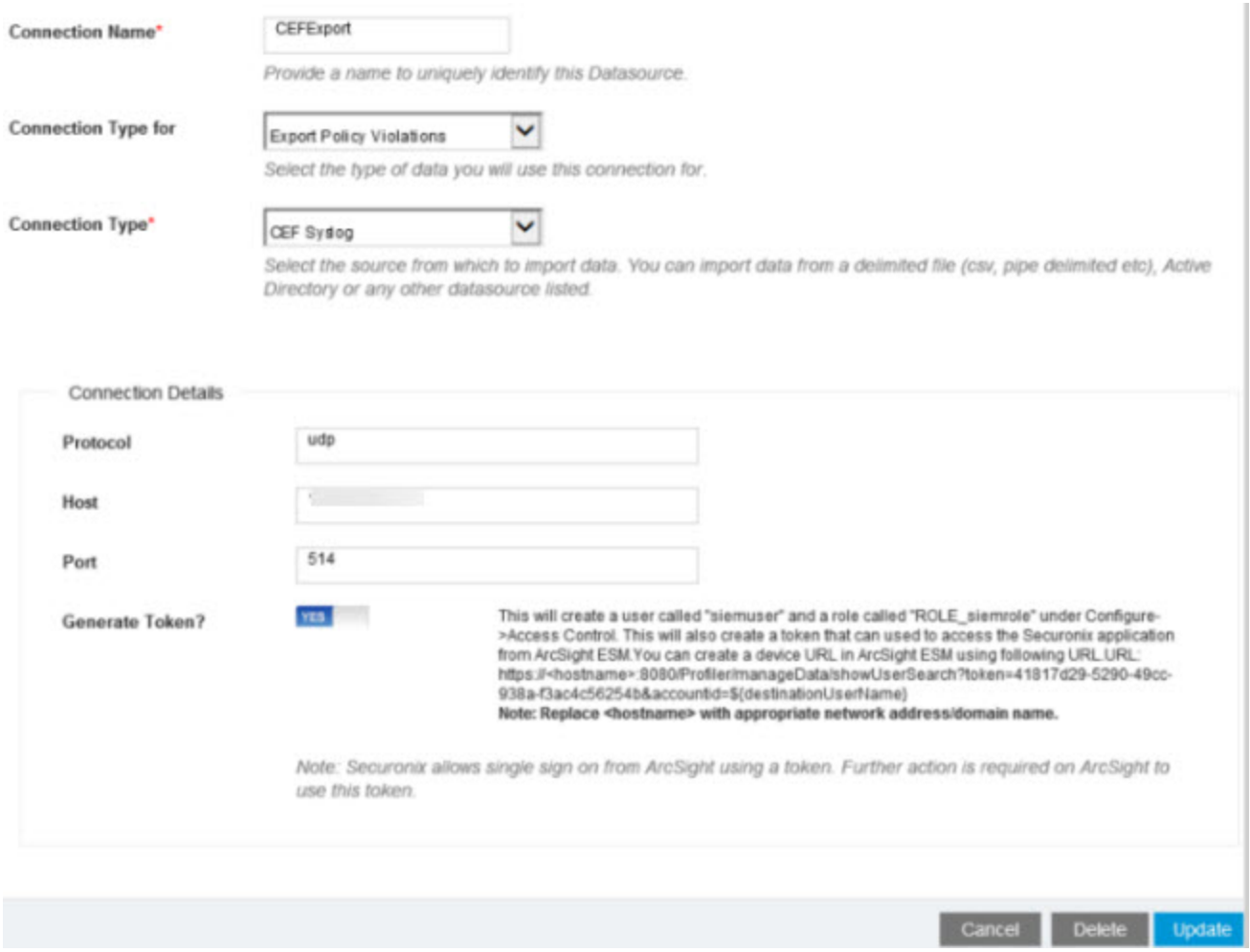
ESM

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

Chapter 2: Creating an HP User Behavior Analytics Token

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

1. From the HP UBA Console, select **Configure** > **Connection Types** .
2. From the Connection Name list, select **CEFExport**
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.



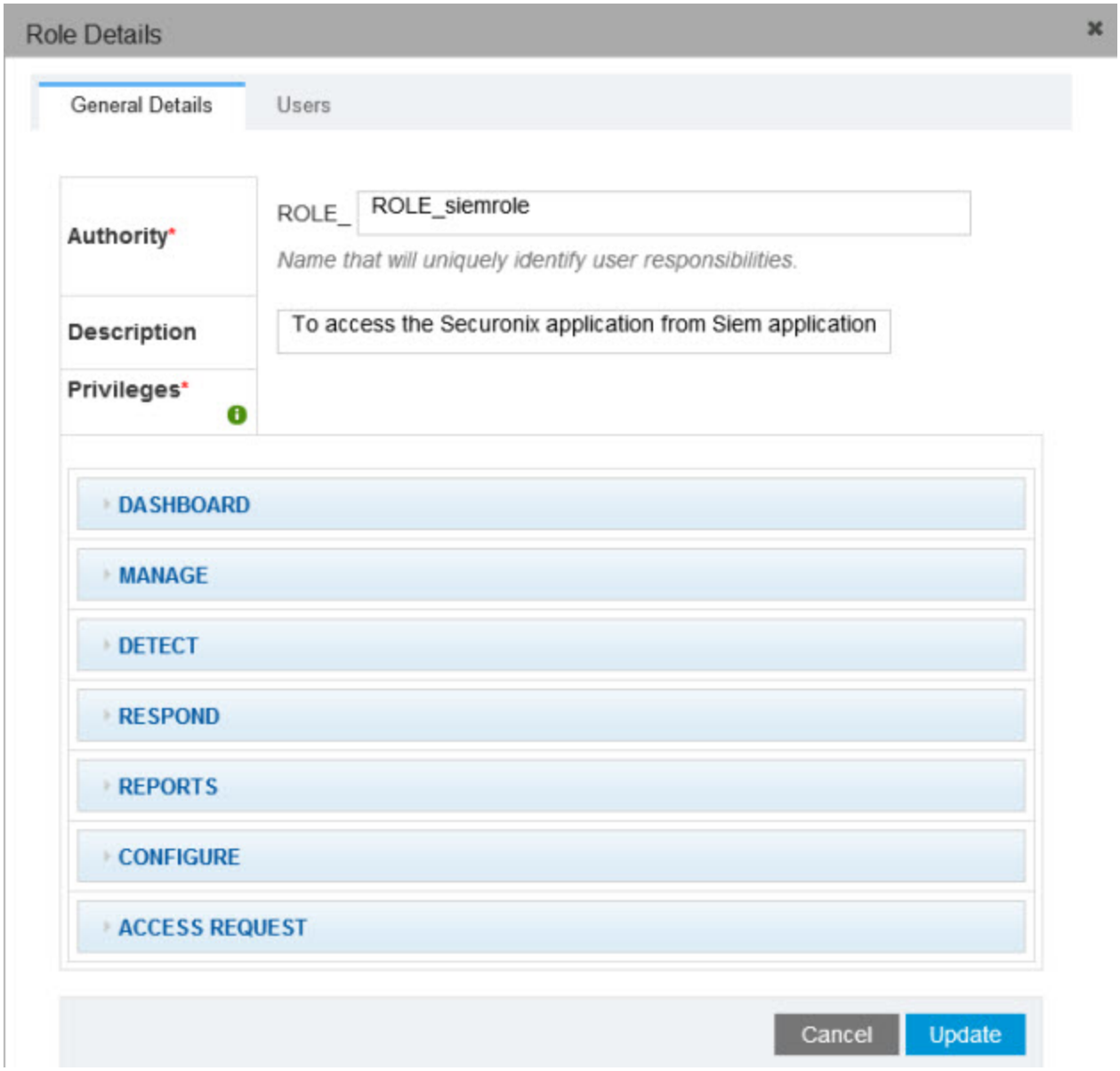
4. Click **Update**.

Creating the token creates a user (siemuser) and a role (ROLE-siemrole). The siemuser must be added to the SECURITYOPERATIONS group:

1. Select **Configure** > **Access Control** > **Manage Users**.
2. Select **siemuser**.
3. Click **Next** > **Next**.
4. Select **SECURITYOPERATIONS**.
5. Click **Next** and **Update**.

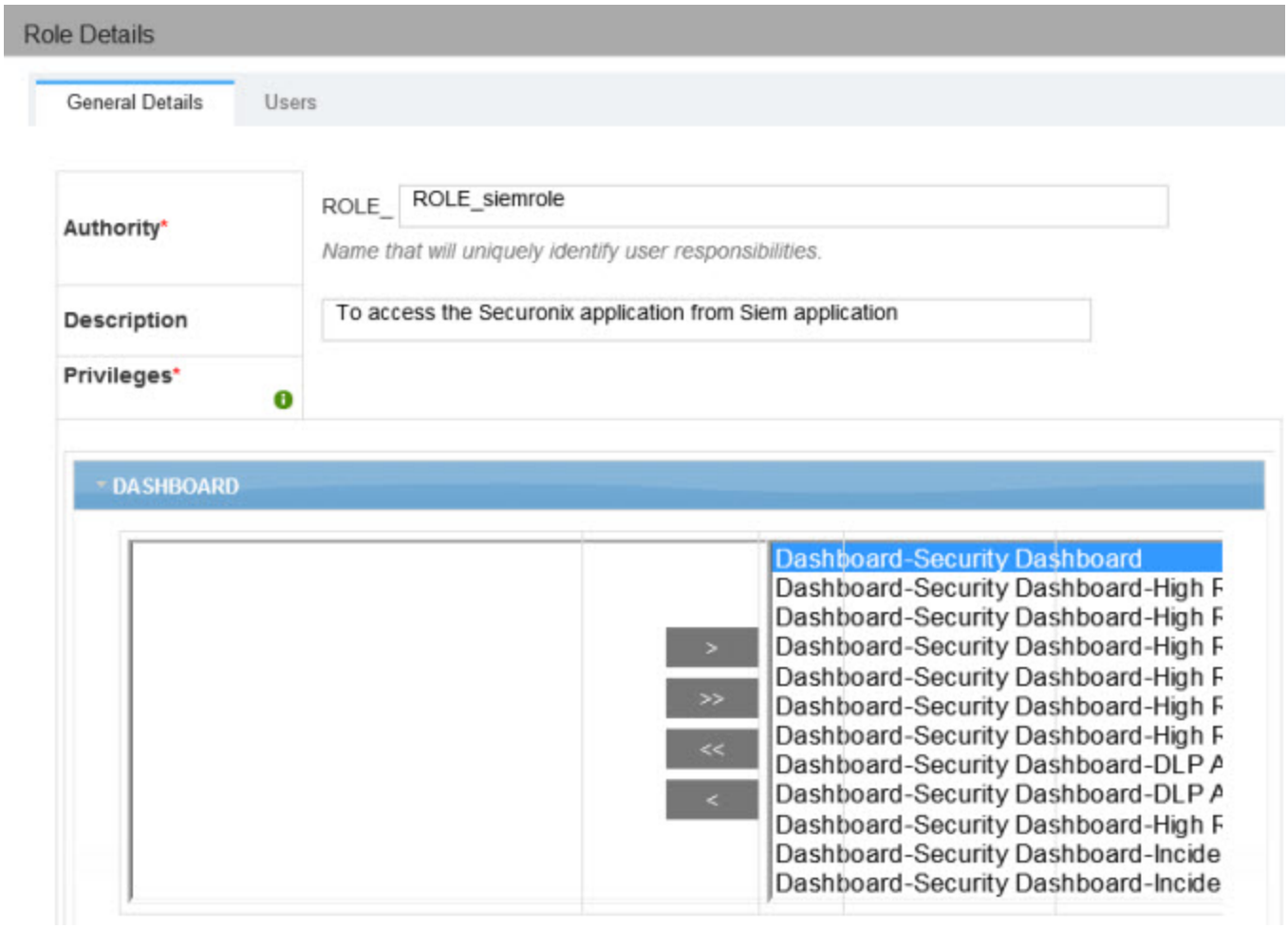
The ROLE_siemrole requires access to all of the HP UBA dashboards. Perform the following procedure to add access to all of the HP UBA dashboards:

1. Select **Configure** > **Access Control** > **Manage Roles**.
2. Click **ROLE_siemrole**.



3. Click **Dashboard**.
4. Click 

to move all of the contents from the left-side box to the right-side box as shown in the following screen:



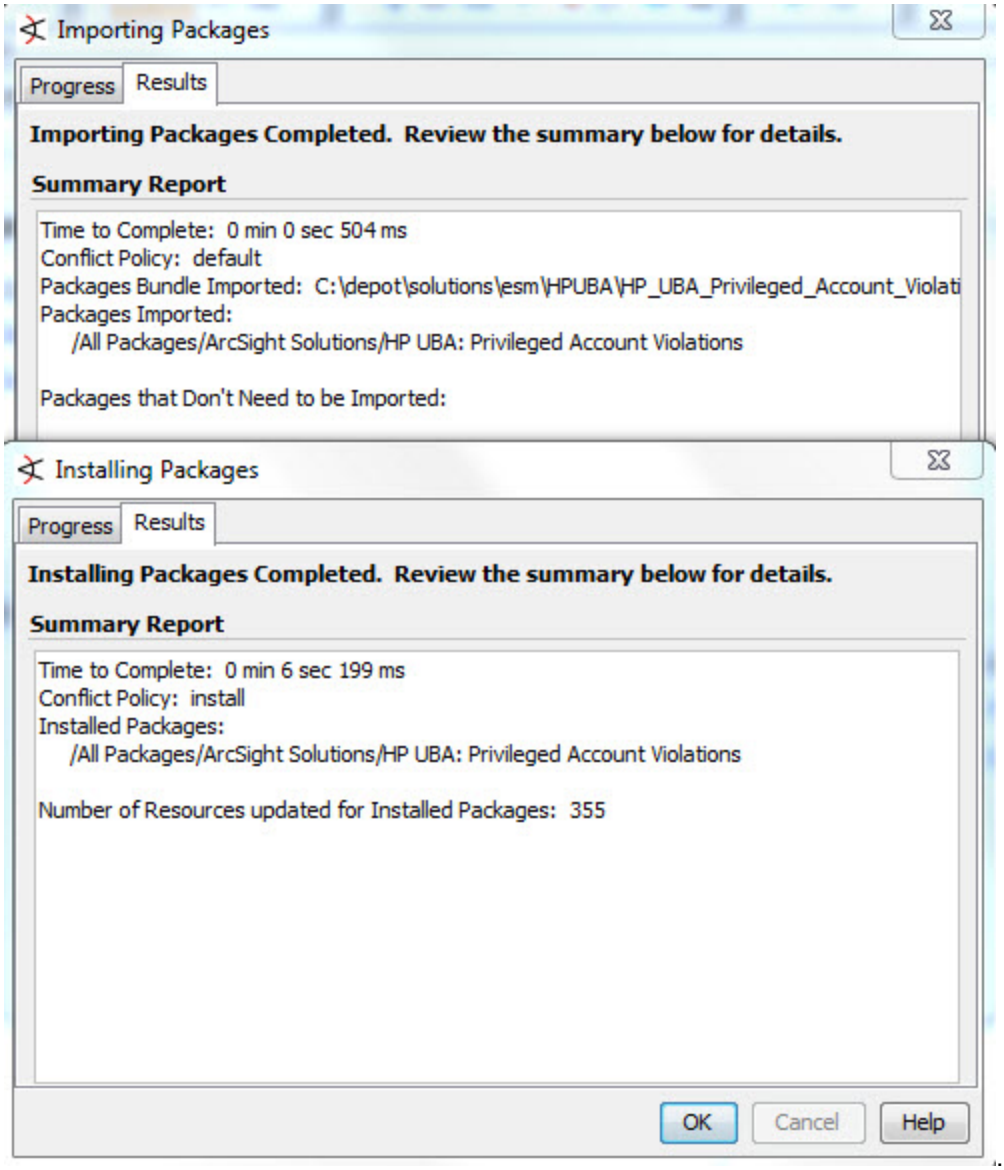
5. Click **Update**.

Chapter 3: Installing the HP User Behavior Analytics Arb File

Use the following procedure to install the HP_UBA_Privileged_Account_Violations_1.0.arb file on ESM:

1. Download the following HP User Behavior Analytics content package bundle to the machine where you plan to run the ArcSight Console: `HP_UBA_Privileged_Account_Violations_1.0.arb`
2. Log into the ArcSight Console with an account that has administrative privileges.
3. In the Navigator panel, click the **Packages** tab.
4. Click **Import**  .
5. 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 Installation dialog, as shown in the following image:

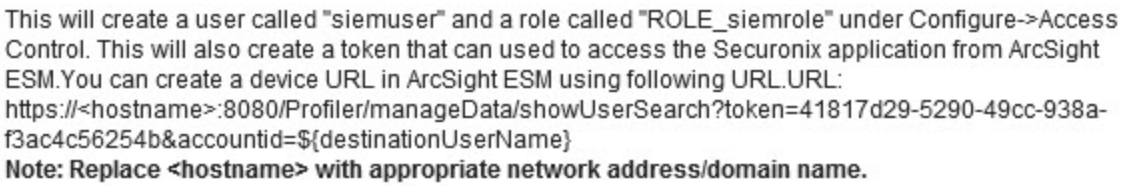


6. In the Packages for Installation dialog, leave the HP User Behavior Analytics checkbox selected and click **Next**.
7. In the Installing Packages dialog, click **OK**.
8. In the Importing Packages dialog, click **OK**.
9. On the Packages tab of the Navigator panel, expand the HP UBA: Privileged Account Violations group to verify that the installation is successful and that the content is accessible in the Navigator panel.

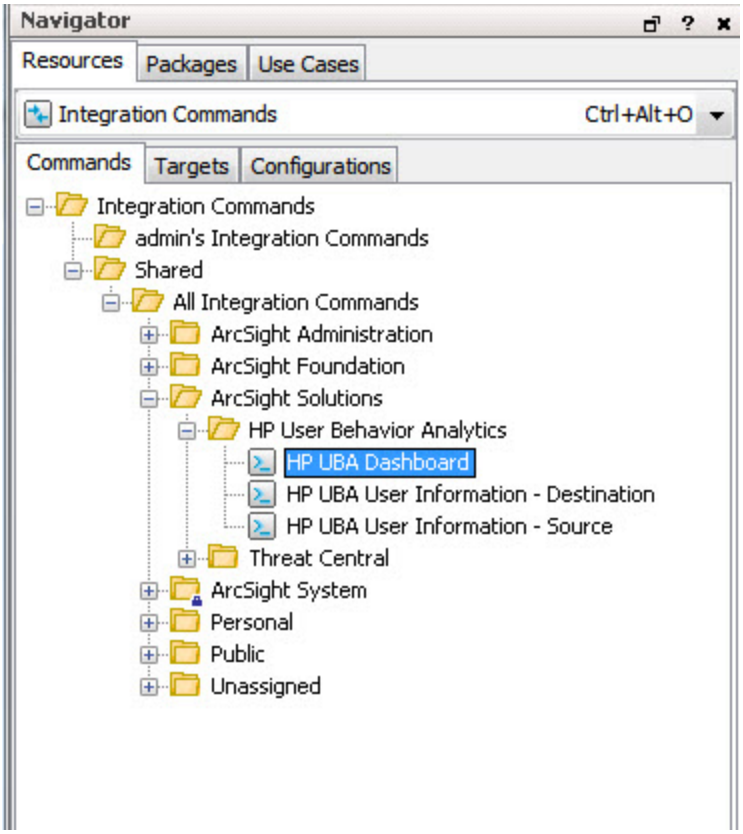
Modifying the HP UBA Dashboard Integration Command

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

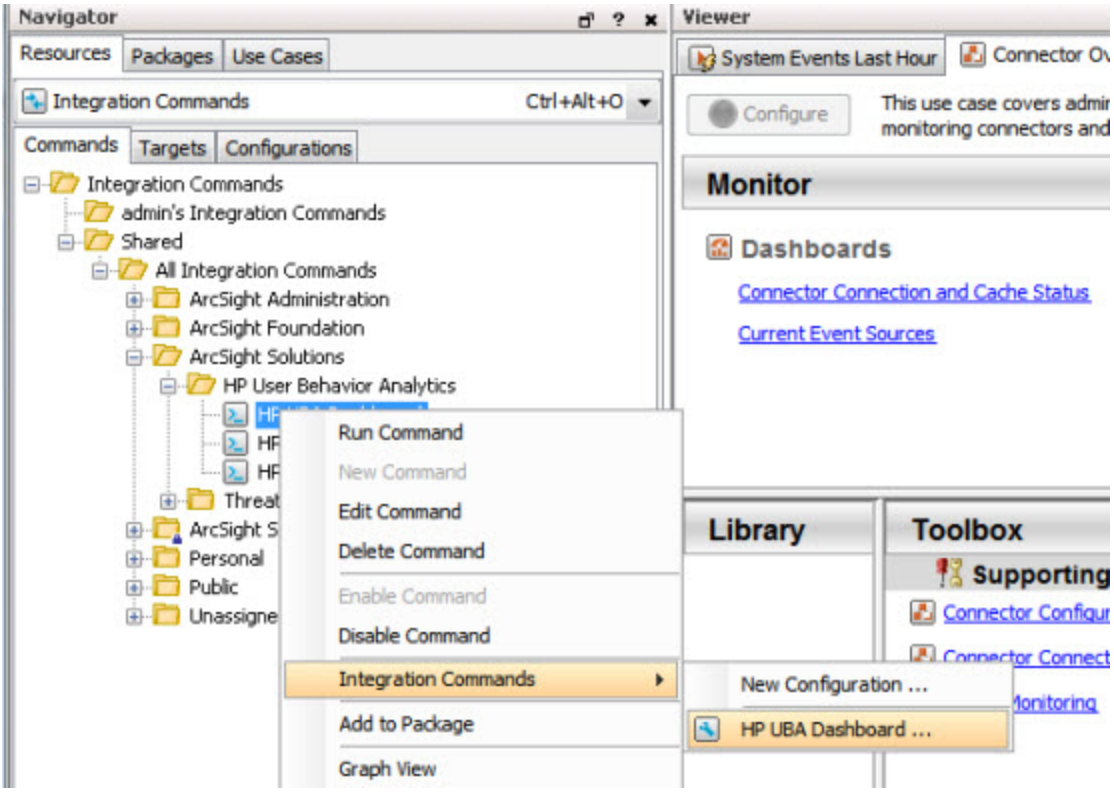
1. Copy the token key (the key follows token=) from the token created in the HP User Behavior Analytics application as shown in the following image:

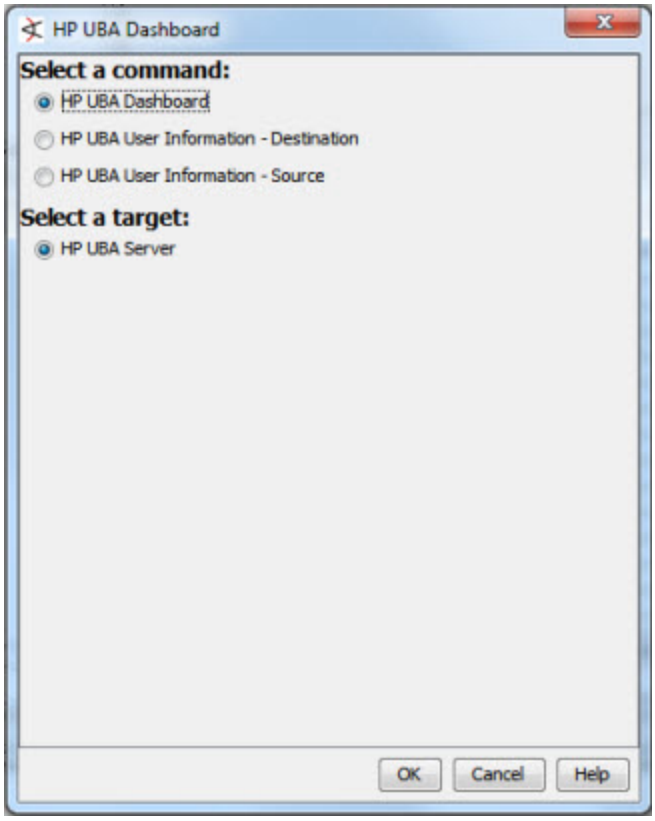
   

2. Log into the ArcSight ESM Console.
3. Select the **Resources** tab and select **Integration Commands** from the drop-down list.
4. Navigate to the HP UBA integration command as shown in the following image:

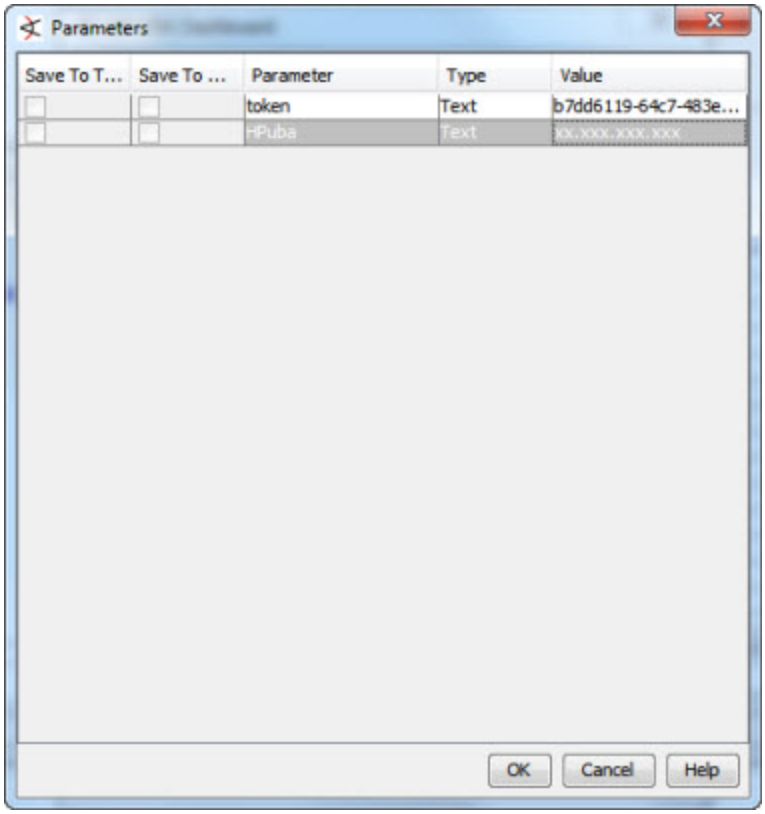


5. Right-click the **HP UBA Dashboard integration command** and select **Integration Commands > HP UBA Dashboard** as shown in the following image:


Navigator
Resources
Packages
Use Cases
Integration Commands
Ctrl+Alt+O
Commands
Targets
Configurations
Integration Commands
admin's Integration Commands
Shared
All Integration Commands
ArcSight Administration
ArcSight Foundation
ArcSight Solutions
HP User Behavior Analytics
Run Command
New Command
Edit Command
Delete Command
Enable Command
Disable Command
Integration Commands
Add to Package
Graph View
New Configuration ...
HP UBA Dashboard ...
Viewer
System Events Last Hour
Configure
Monitor
Dashboards
Connector Connection and Cache Status
Current Event Sources
Library
Toolbox
Supporting



6. Select HP UBA Dashboard for the command and HP UBA Server as the target. Click **OK**.



7. In the token Value field, paste the token key. In the HPuba Value field, enter the IP address or host name of the HP User Behavior Analytics server.
8. Click the **Save To Target** checkbox for both parameters. Once saved, you do not have enter either parameter again.
9. 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.

Configuring a Logger Receiver

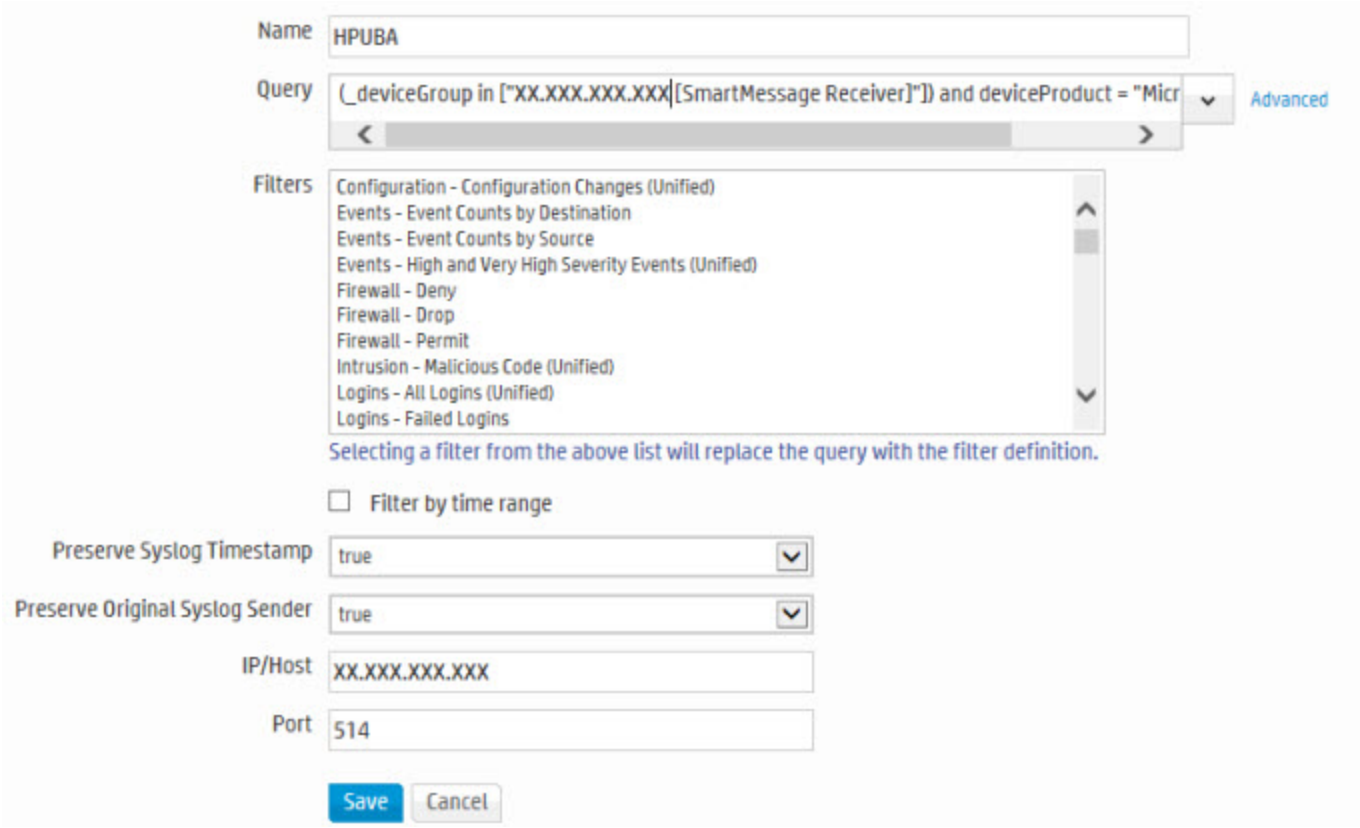
Perform the following procedure to configure a Logger receiver:

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 User Behavior Analytics:

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**. The following screen displays:



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 HP UBA runs.
   - **Port** - Enter the port where events should be sent to the machine where HP UBA runs.

7. Click **Save**.

Chapter 5: Using a SmartConnector to Send Events to Logger

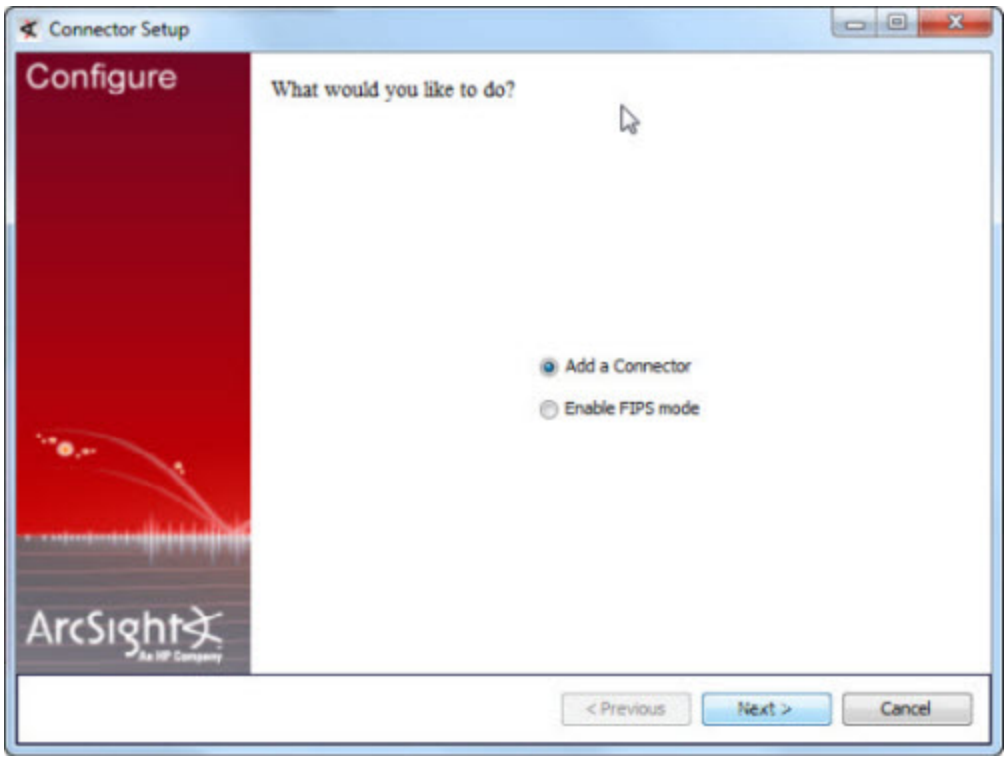
Logger comes pre-configured with a SmartMessage Receiver. You can also create and configure new SmartMessage Receivers for multiple connector inputs to Logger. Configure the Logger receiver before configuring the connector so that the receiver name, port and output type are set prior to configuring the connector. See "Creating and Configuring Logger Receivers and Forwarder" on page 20 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.

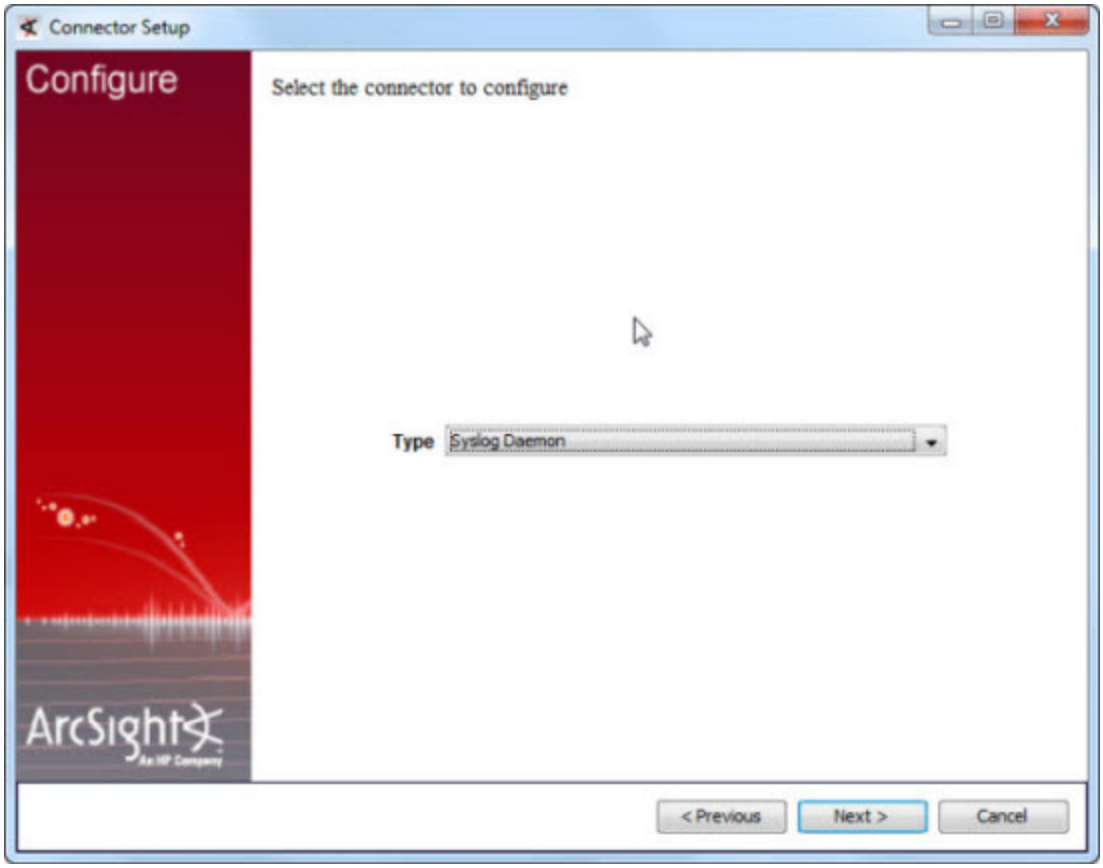
Configuring a Connector to Send Syslog CEF Events

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

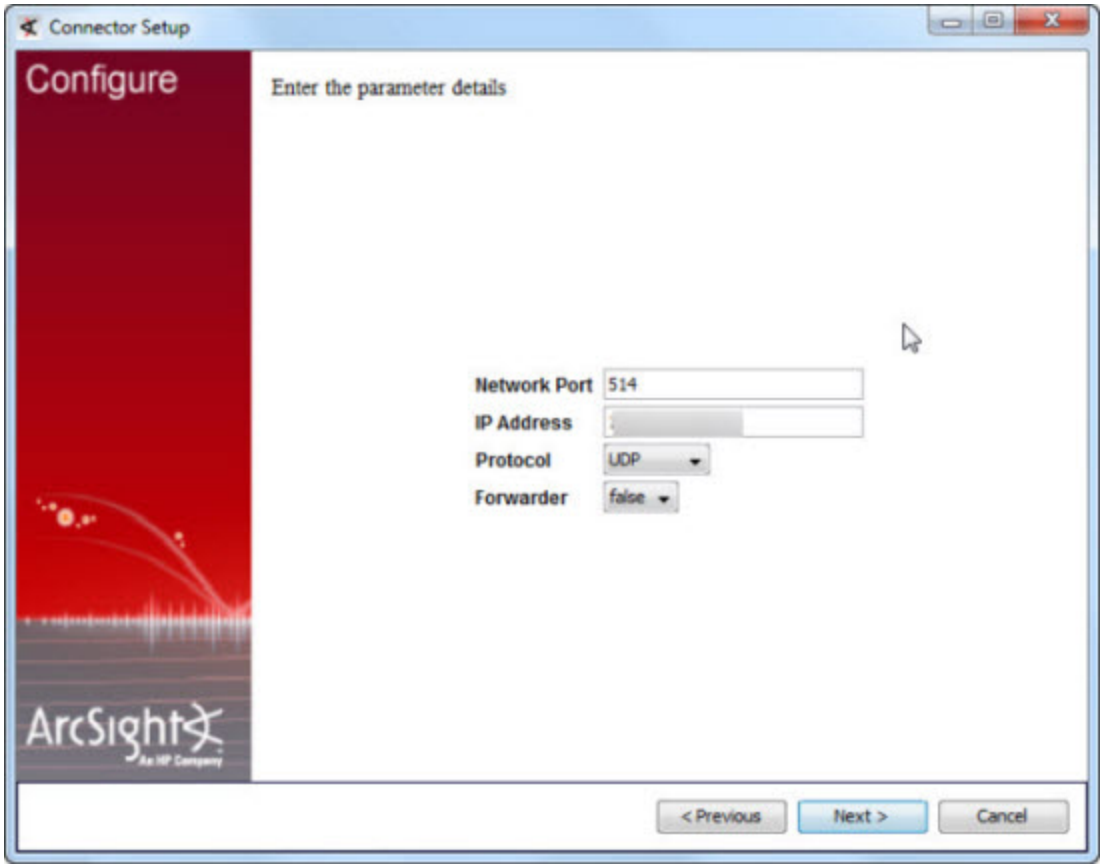
1. Run the AcrSight SmartConnector Installer.



2. Select **Add a Connector**. Click **Next**.

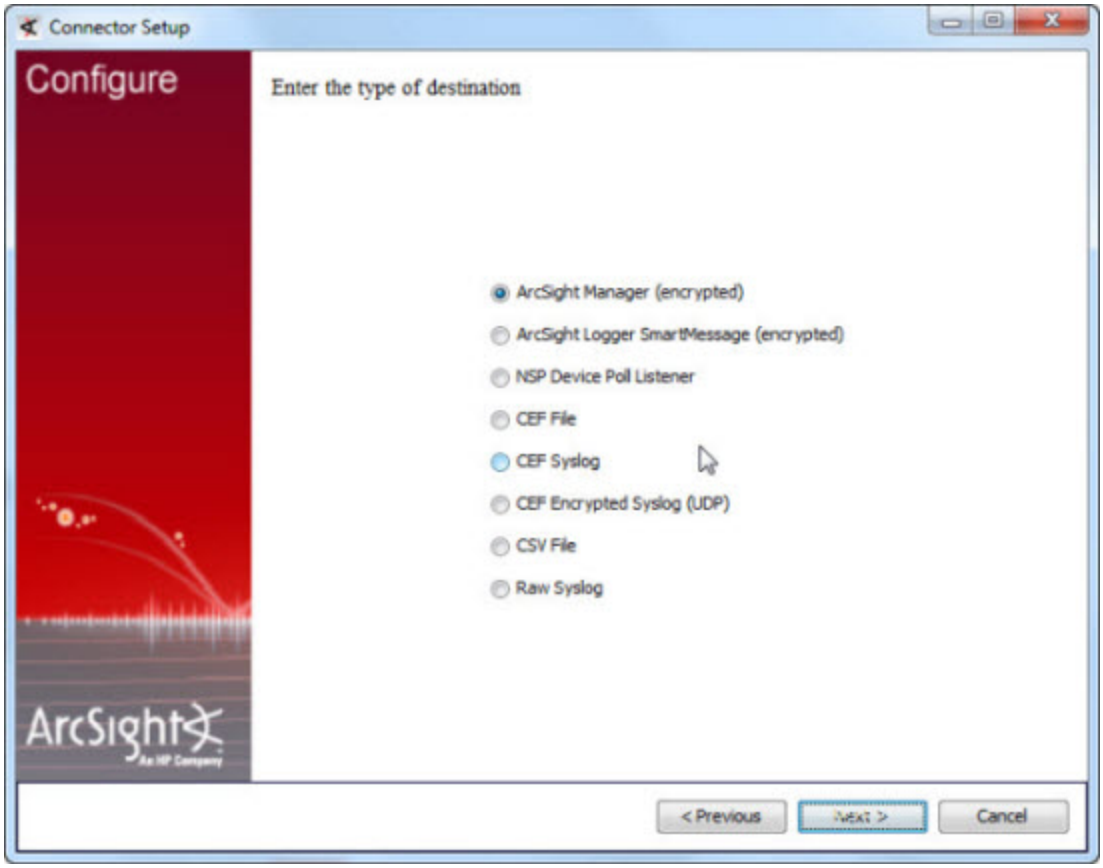


3. Select **Syslog Daemon**. Click **Next**.

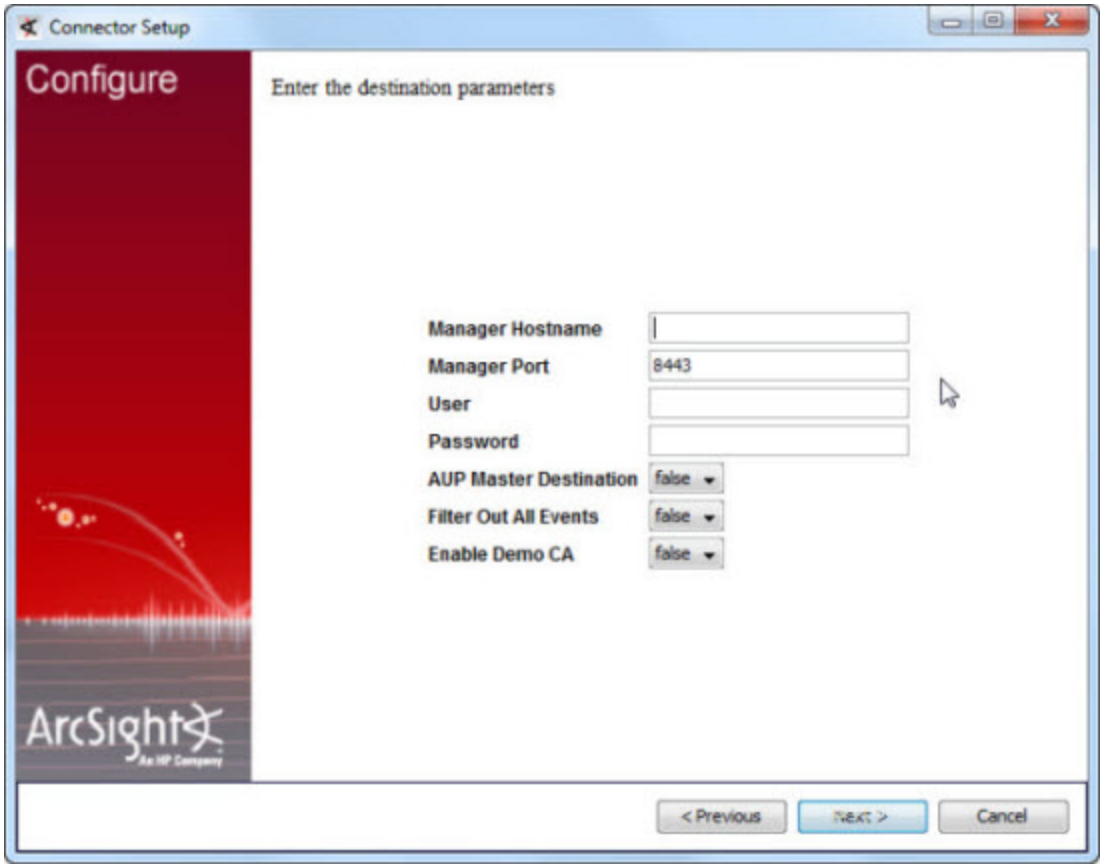


4. Enter values for the following parameters:

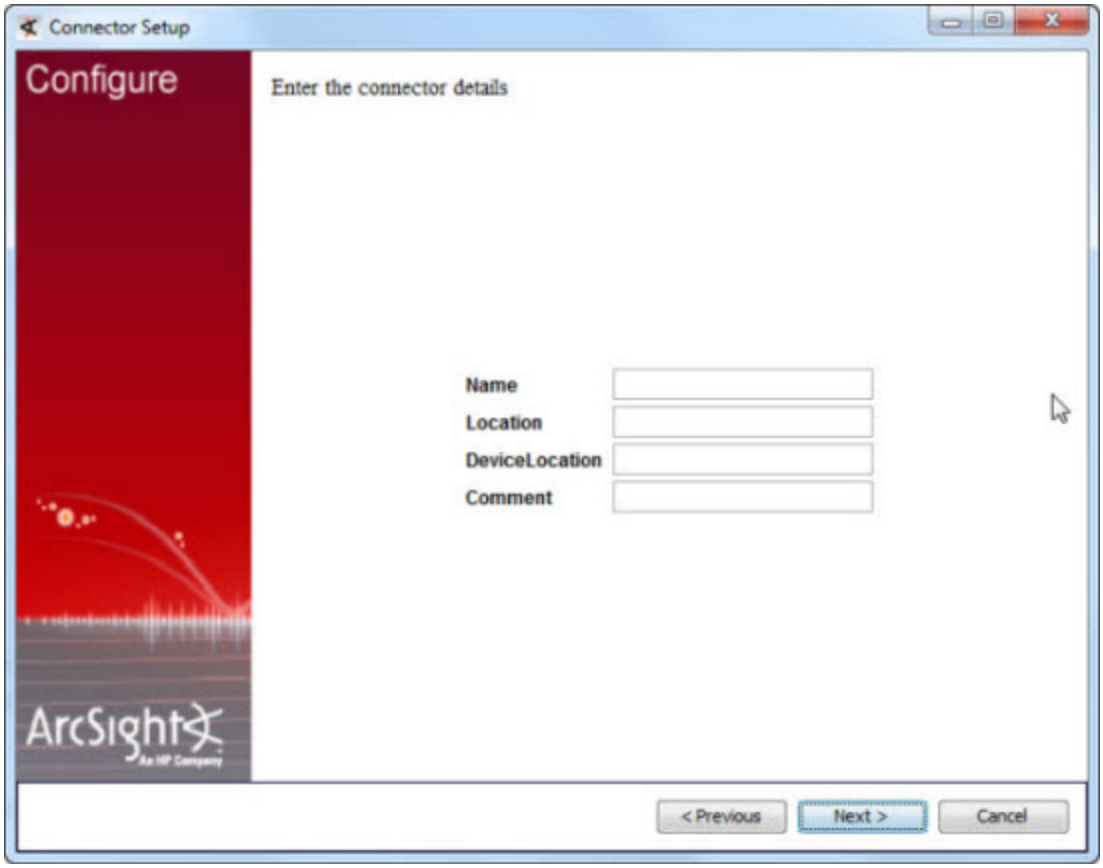
   - **Network Port** - 514
   - **IP Address** - for the connector
   - **Protocol** - UDP
   - Forwarder - **False**
     Click **Next**.



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**.

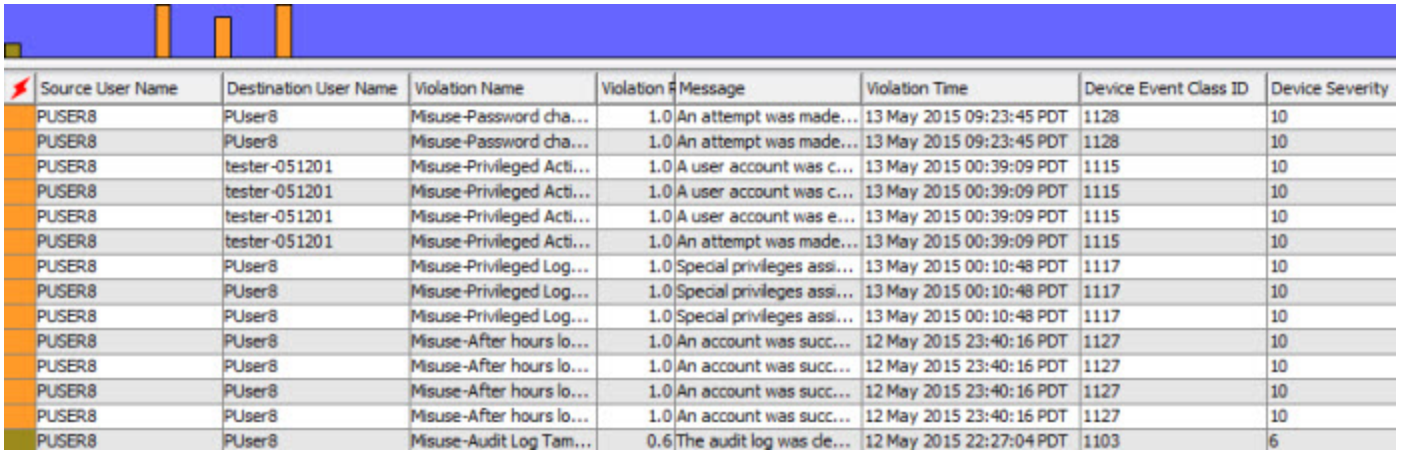
9. Complete the installation.

Chapter 6: Use Case Overview

HP User Behavior Analytics provides two use cases:

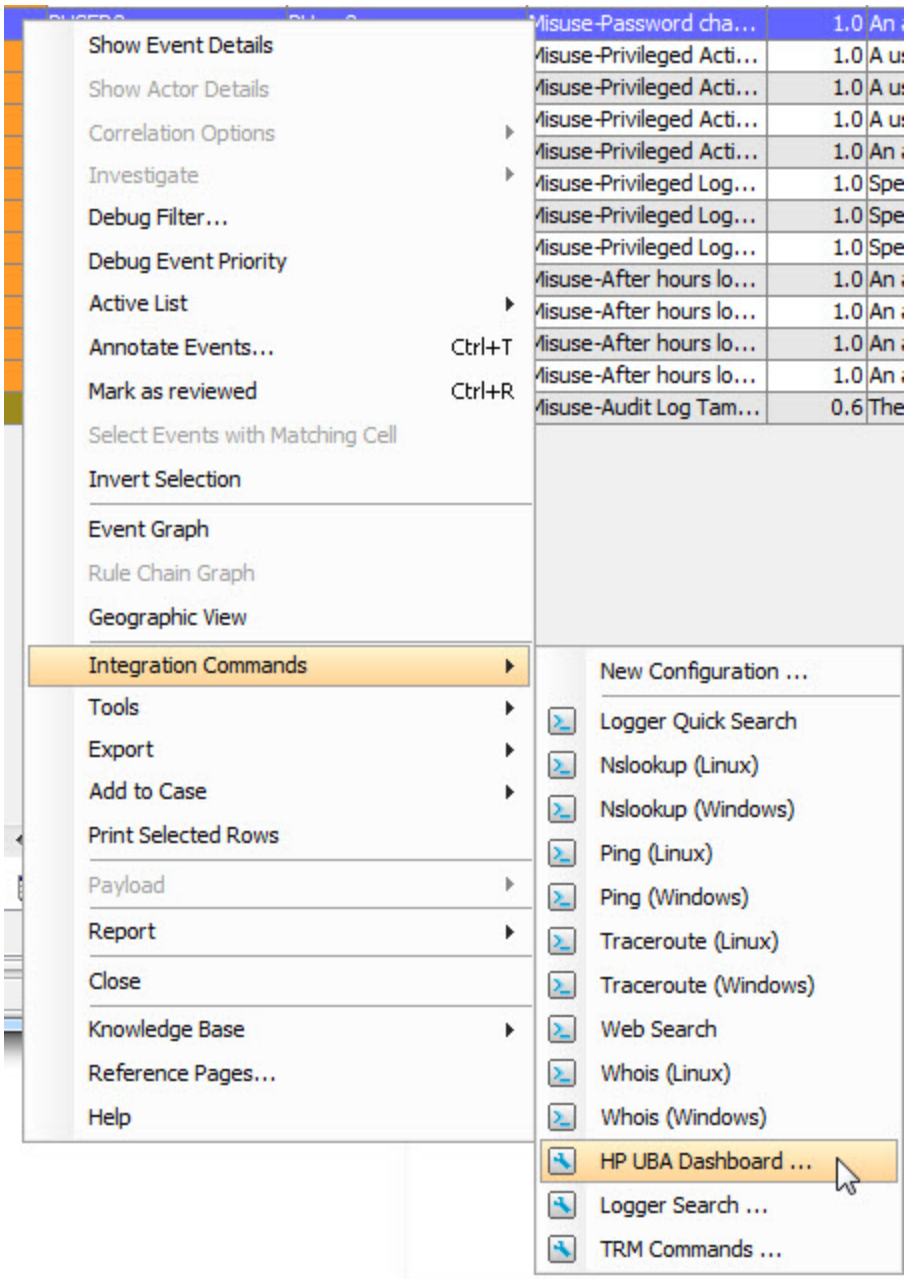
- Privileged Account Access Violations Monitoring - monitors access violations to privileged accounts
- Privileged Account Action Violations Monitoring - monitors unauthorized actions to privileged accounts

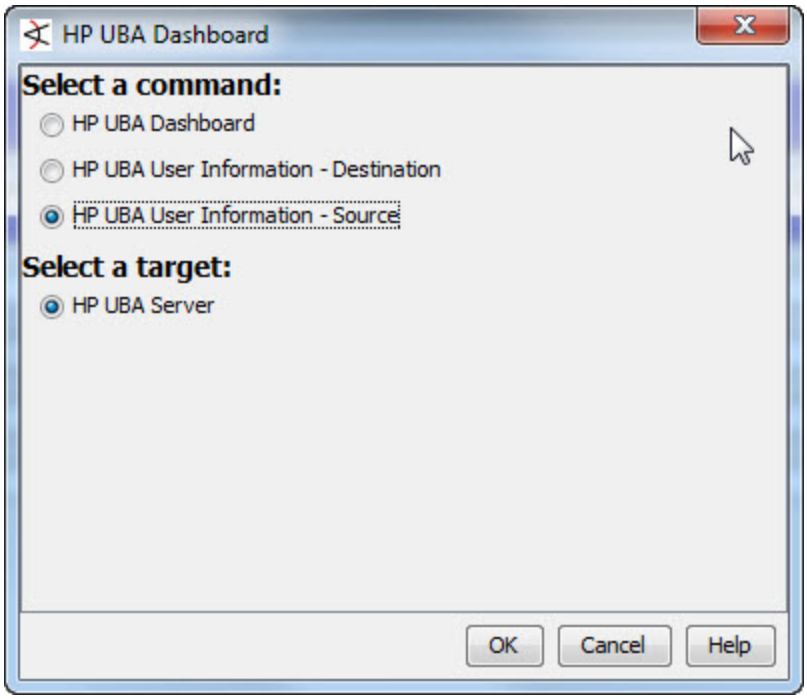
The integration between HP UBA and ESM is accomplished using integration commands. The integration commands are designed to work primarily with the active channels. For example, a partial view of the Privileged Account Violations Active Channel might have the following information:



Source User Name	Destination User Name	Violation Name	Violation F	Message	Violation Time	Device Event Class ID	Device Severity
PUSER8	PUser8	Misuse-Password cha...	1.0	An attempt was made...	13 May 2015 09:23:45 PDT	1128	10
PUSER8	PUser8	Misuse-Password cha...	1.0	An attempt was made...	13 May 2015 09:23:45 PDT	1128	10
PUSER8	tester-051201	Misuse-Privileged Acti...	1.0	A user account was c...	13 May 2015 00:39:09 PDT	1115	10
PUSER8	tester-051201	Misuse-Privileged Acti...	1.0	A user account was c...	13 May 2015 00:39:09 PDT	1115	10
PUSER8	tester-051201	Misuse-Privileged Acti...	1.0	A user account was e...	13 May 2015 00:39:09 PDT	1115	10
PUSER8	tester-051201	Misuse-Privileged Acti...	1.0	An attempt was made...	13 May 2015 00:39:09 PDT	1115	10
PUSER8	PUser8	Misuse-Privileged Log...	1.0	Special privileges assi...	13 May 2015 00:10:48 PDT	1117	10
PUSER8	PUser8	Misuse-Privileged Log...	1.0	Special privileges assi...	13 May 2015 00:10:48 PDT	1117	10
PUSER8	PUser8	Misuse-Privileged Log...	1.0	Special privileges assi...	13 May 2015 00:10:48 PDT	1117	10
PUSER8	PUser8	Misuse-After hours lo...	1.0	An account was succ...	12 May 2015 23:40:16 PDT	1127	10
PUSER8	PUser8	Misuse-After hours lo...	1.0	An account was succ...	12 May 2015 23:40:16 PDT	1127	10
PUSER8	PUser8	Misuse-After hours lo...	1.0	An account was succ...	12 May 2015 23:40:16 PDT	1127	10
PUSER8	PUser8	Misuse-After hours lo...	1.0	An account was succ...	12 May 2015 23:40:16 PDT	1127	10
PUSER8	PUser8	Misuse-Audit Log Tam...	0.6	The audit log was de...	12 May 2015 22:27:04 PDT	1103	6

You can select an event, then right-click the event and select Integration Commands > HP UBA Dashboard:

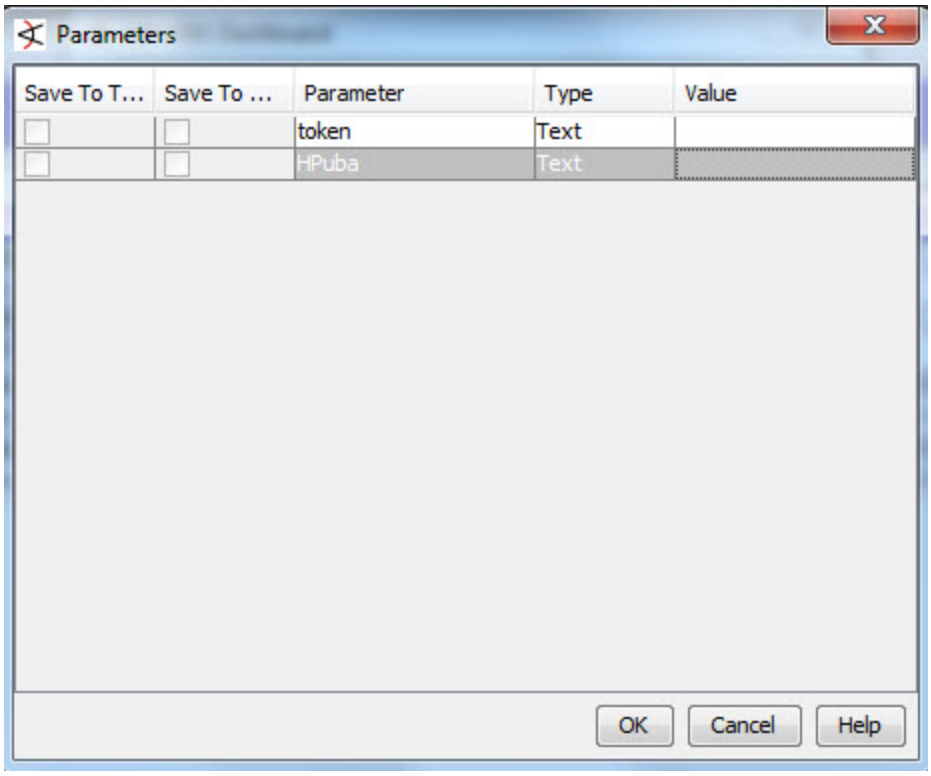

Misuse-Password cha... 1.0
Misuse-Privileged Acti... 1.0
Misuse-Privileged Acti... 1.0
Misuse-Privileged Acti... 1.0
Misuse-Privileged Acti... 1.0
Misuse-Privileged Log... 1.0
Misuse-Privileged Log... 1.0
Misuse-Privileged Log... 1.0
Misuse-After hours lo... 1.0
Misuse-After hours lo... 1.0
Misuse-After hours lo... 1.0
Misuse-After hours lo... 1.0
Misuse-Audit Log Tam... 0.6
Show Event Details
Show Actor Details
Correlation Options
Investigate
Debug Filter...
Debug Event Priority
Active List
Annotate Events... Ctrl+T
Mark as reviewed Ctrl+R
Select Events with Matching Cell
Invert Selection
Event Graph
Rule Chain Graph
Geographic View
Integration Commands
Tools
Export
Add to Case
Print Selected Rows
Payload
Report
Close
Knowledge Base
Reference Pages...
Help
New Configuration ...
Logger Quick Search
Nslookup (Linux)
Nslookup (Windows)
Ping (Linux)
Ping (Windows)
Traceroute (Linux)
Traceroute (Windows)
Web Search
Whois (Linux)
Whois (Windows)
HP UBA Dashboard ...
Logger Search ...
TRM Commands ...



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

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

For the HP UBA Dashboard dialog above, clicking OK displays the Parameters dialog:



In the HPuba value field, enter the IP address for the HP UBA server and click **OK**. You will be linked to the General Details page in HP 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

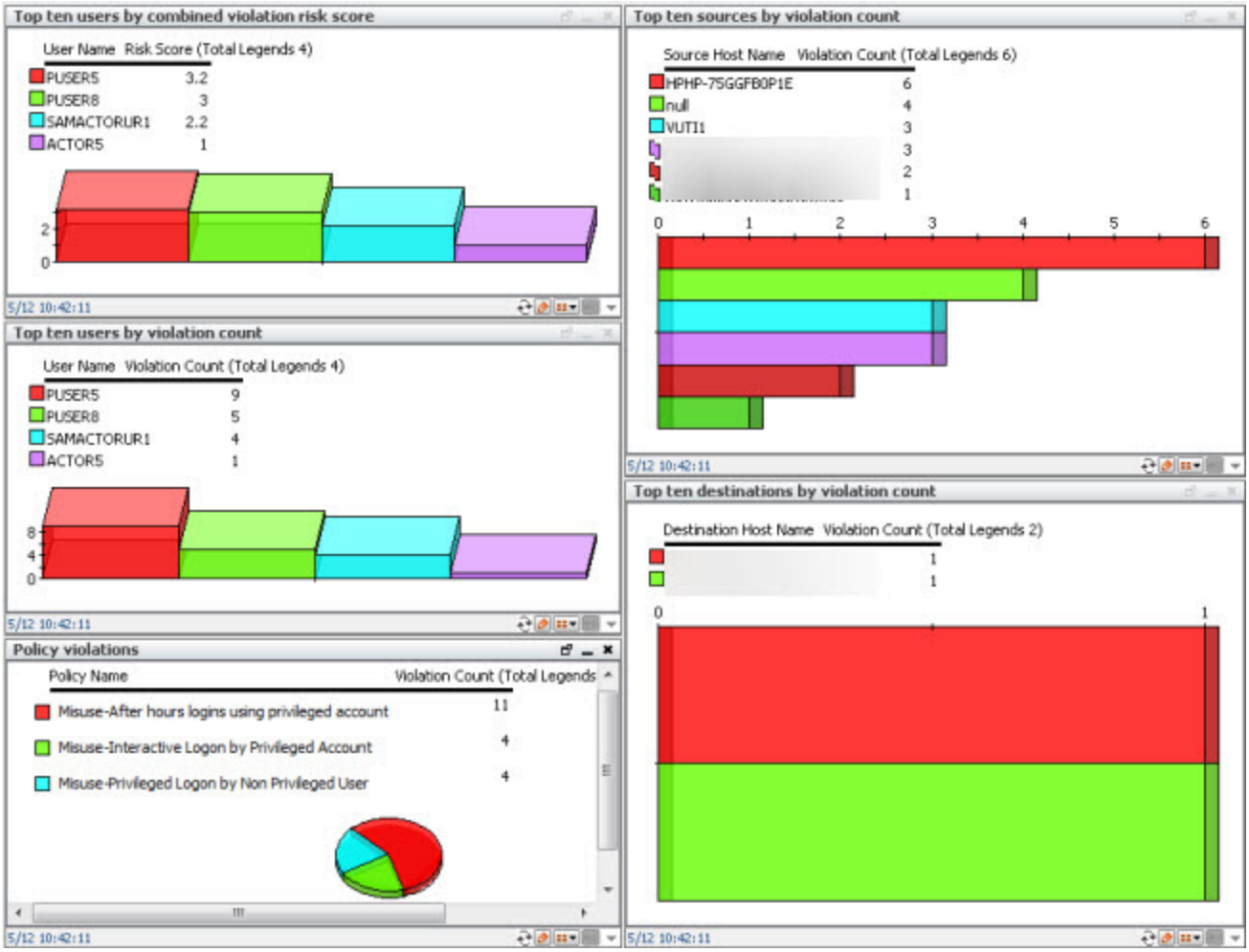
- Peer Groups
- Monitor Access
- Monitor Activities
- Behavior Profile

The HP UBA User Information - Destination integration command is configured like the HP 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 HP User Behavior Analytics. This use case has one rule that is triggered when a violation is received from HP 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

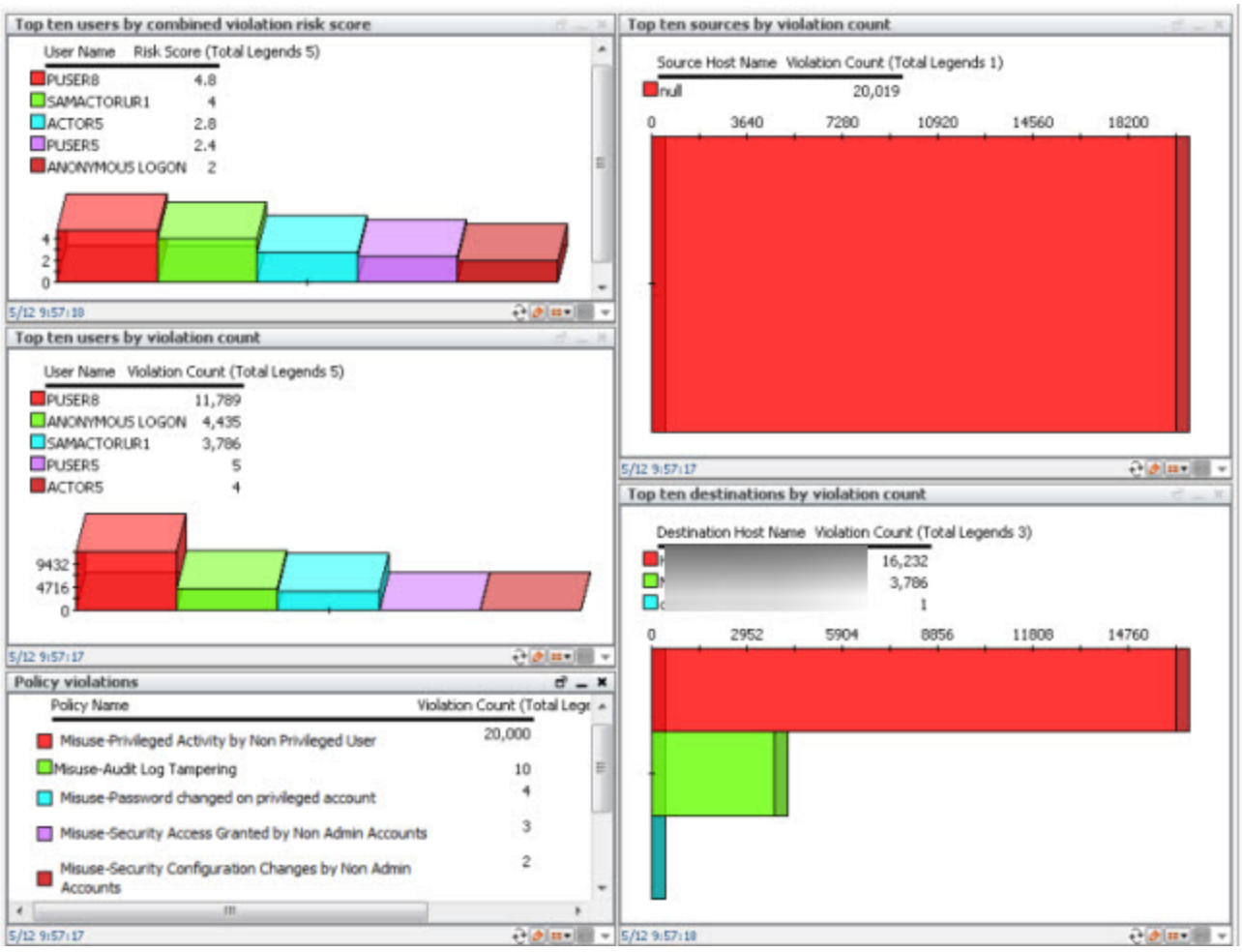
For information about all the resources for this use case, see "HP User Behavior Analytics Resources By Type".

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 HP User Behavior Analytics. This use case has one rule that is triggered when a violation is received from HP 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 "HP 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: HP User Behavior Analytics Resources By Type

This appendix lists all the HP User Behavior Analytics resources by type.

Active Channels

The following table lists all the active channels.

Active Channels Resources

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

Active Lists

The following table lists all the 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 Violations rule.	`/All Active Lists/ArcSight Solutions/HP User Behavior Analytics/`

Dashboards

The following table lists all the dashboards.

Dashboards Resources

Resource	Description	URI
Privileged action violations	This dashboard shows privileged action violations details sorted by the violation time (latest first).	`/All Dashboards/ArcSight Solutions/HP User Behavior Analytics/Privileged Action Violations/`

Dashboards Resources, continued

Resource	Description	URI
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/HP User Behavior Analytics/Privileged Action Violations/`
Privileged login violations	This dashboard shows privileged login violation details sorted by the violation time (latest first).	`/All Dashboards/ArcSight Solutions/HP User Behavior Analytics/Privileged Account Login Violations/`

Dashboards Resources, continued

Resource	Description	URI
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/HP User Behavior Analytics/Privileged Account Login Violations/`

Field Sets

The following table lists all the 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/HP User Behavior Analytics/`

Filters

The following table lists all the filters.

Filters Resources

Resource	Description	URI
Privileged Account Violations	This filter identifies HP UBA privileged account violation events.	`/All Filters/ArcSight Solutions/HP User Behavior Analytics/`

Integration Commands

The following table lists all the integration commands.

Integration Commands Resources

Resource	Description	URI
HP UBA Dashboard	This integration command connects to the HP UBA Dashboard web page as the SIEMUser in Securonix. The "SIEMUser" must have admin or full dashboard privileges in Securonix or this command will fail.	`/All Integration Commands/ArcSight Solutions/HP User Behavior Analytics/`
HP UBA User Information - Destination	With a right-click on an event in the Active Channel, this integration command connects to the HP UBA web page and displays the details for the Destination User Name.	`/All Integration Commands/ArcSight Solutions/HP User Behavior Analytics/`
HP UBA User Information - Source	With a right-click on an event in the Active Channel, this integration command connects to the HP UBA web page and displays details for the Source User Name.	`/All Integration Commands/ArcSight Solutions/HP User Behavior Analytics/`

Integration Configurations

The following table lists all the integration configurations.

Integration Configurations Resources

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

Integration Targets

The following table lists all the integration targets.

Integration Targets Resources

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

Queries

The following table lists all the 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/HP User Behavior Analytics/Privileged Account Login Violations/`

Queries Resources, continued

Resource	Description	URI
Audit Log Tampering	This query selects information about audit log tampering activity.	/All Queries/ArcSight Solutions/HP 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 privileged accounts list maintained by HP UBA.	/All Queries/ArcSight Solutions/HP User Behavior Analytics/Privileged Action 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/HP User Behavior Analytics/Privileged Account Login 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/HP User Behavior Analytics/Privileged Action Violations/
Privileged Activities by Unauthorized User	This query selects information about privileged activity by unauthorized users. For example, when privileged activity by an unauthorized user is detected.	/All Queries/ArcSight Solutions/HP User Behavior Analytics/Privileged Action Violations/
Privileged Logins by Unauthorized User	This query selects information about privileged account logins by unauthorized users.For example, when an unauthorized user attempts to login to an account with privileged access.	/All Queries/ArcSight Solutions/HP User Behavior Analytics/Privileged Account Login Violations/
Security Access Granted by Unauthorized Account	This query selects information about violation activity when a user is granted security access by an unauthorized account.	/All Queries/ArcSight Solutions/HP User Behavior Analytics/Privileged Action Violations/

Queries Resources, continued

Resource	Description	URI
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/HP User Behavior Analytics/Privileged Action Violations/
Service Account Interactive Logins	This query selects information about successful interactive logins by accounts tagged as service accounts.	/All Queries/ArcSight Solutions/HP User Behavior Analytics/Privileged Account Login Violations/
Top ten destinations by violation count	This query selects information about the top ten destinations ranked by the count of login violations targeted at a destination.	/All Queries/ArcSight Solutions/HP User Behavior Analytics/Privileged Account Login Violations/
Top ten destinations by violation count	This query selects information about the top ten destinations ranked by the count of action violations targeted at a destination.	/All Queries/ArcSight Solutions/HP User Behavior Analytics/Privileged Action Violations/
Top ten sources by violation count	This query selects information about the top ten sources ranked by the count of login violations originated from a source.	/All Queries/ArcSight Solutions/HP User Behavior Analytics/Privileged Account Login Violations/
Top ten sources by violation count	This query selects information about the top ten sources ranked by the count of action violations originated from a source.	/All Queries/ArcSight Solutions/HP User Behavior Analytics/Privileged Action 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/HP User Behavior Analytics/Privileged Account Login Violations/

Queries Resources, continued

Resource	Description	URI
Top ten users by combined violatoin risk score	This query selects information about the top ten users ranked by the user action violations combined risk score.	`/All Queries/ArcSight Solutions/HP User Behavior Analytics/Privileged Action Violations/`
Top ten users by violation count	This query selects information about the top ten users ranked by the combined login violation count.	`/All Queries/ArcSight Solutions/HP User Behavior Analytics/Privileged Account Login Violations/`
Top ten users by violation count	This query selects information about the top ten users ranked by the combined action violation count.	`/All Queries/ArcSight Solutions/HP User Behavior Analytics/Privileged Action Violations/`
User Activity Details	This query selects information about policy violation details. It is used in drilldowns for the privileged user activity dashboards.	`/All Queries/ArcSight Solutions/HP User Behavior Analytics/`

Query Viewers

The following table lists all the 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/HP User Behavior Analytics/Privileged Account Login Violations/`
Audit Log Tampering	This query viewer shows audit log tampering activity.	`/All Query Viewers/ArcSight Solutions/HP User Behavior Analytics/Privileged Action Violations/`

Query Viewers Resources, continued

Resource	Description	URI
Password Changes on a Privileged Account	This query viewer shows the password changes for accounts in the privileged accounts list maintained by HP UBA.	/All Query Viewers/ArcSight Solutions/HP User Behavior Analytics/Privileged Action Violations/
Policy violations	This query viewer shows privileged account login policy violations with the number of times each type of violation occurred.	/All Query Viewers/ArcSight Solutions/HP User Behavior Analytics/Privileged Account Login 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/HP User Behavior Analytics/Privileged Action Violations/
Privileged Activities by Unauthorized User	This query viewer shows privileged activities by unauthorized users. This happens when a privileged activity by an unauthorized user is detected.	/All Query Viewers/ArcSight Solutions/HP User Behavior Analytics/Privileged Action Violations/
Privileged Logins by Unauthorized User	This query viewer shows privileged account logins by unauthorized users.	/All Query Viewers/ArcSight Solutions/HP User Behavior Analytics/Privileged Account Login Violations/
Security Access Granted by Unauthorized Account	This query viewer shows the activity violation of an unauthorized user granting security access to another user.	/All Query Viewers/ArcSight Solutions/HP User Behavior Analytics/Privileged Action Violations/
Security Configuration Changes Made by Unauthorized Account	This query viewer shows an activity violation when security configuration changes are made by an unauthorized user.	/All Query Viewers/ArcSight Solutions/HP User Behavior Analytics/Privileged Action Violations/
Service Account Interactive Logins	This query viewer shows successful interactive logins by accounts tagged as service accounts.	/All Query Viewers/ArcSight Solutions/HP User Behavior Analytics/Privileged Account Login Violations/

Query Viewers Resources, continued

Resource	Description	URI
Top ten destinations by violation count	This query viewer shows the top ten destinations ranked by the count of login violations targeted to each destination.	/All Query Viewers/ArcSight Solutions/HP User Behavior Analytics/Privileged Account Login Violations/
Top ten destinations by violation count	This query viewer shows the top ten destinations ranked by the count of action violations targeted to each destination.	/All Query Viewers/ArcSight Solutions/HP User Behavior Analytics/Privileged Action Violations/
Top ten sources by violation count	This query viewer shows the top ten sources ranked by the count of login violations originated from each source.	/All Query Viewers/ArcSight Solutions/HP User Behavior Analytics/Privileged Account Login Violations/
Top ten sources by violation count	This query viewer shows the top ten sources ranked by the count of action violations originated from each source.	/All Query Viewers/ArcSight Solutions/HP User Behavior Analytics/Privileged Action Violations/
Top ten users by combined violation risk score	This query viewer shows the top ten users ranked by the user login violation combined risk score.	/All Query Viewers/ArcSight Solutions/HP User Behavior Analytics/Privileged Account Login Violations/
Top ten users by combined violation risk score	This query viewer shows the top ten users ranked by the user action violation combined risk score.	/All Query Viewers/ArcSight Solutions/HP User Behavior Analytics/Privileged Action Violations/
Top ten users by violation count	This query viewer shows the top ten users ranked by the combined login violation count.	/All Query Viewers/ArcSight Solutions/HP User Behavior Analytics/Privileged Account Login Violations/
Top ten users by violation count	This query viewer shows the top ten users ranked by the combined action violation count.	/All Query Viewers/ArcSight Solutions/HP 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/HP User Behavior Analytics/

Rules

The following table lists all the rules.

Rules Resources

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

Use Cases

The following table lists all the 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/HP 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/HP 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 HP User Behavior Analytics Integration and Content Guide (User Behavior Analytics 1.0)

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@hp.com.

We appreciate your feedback!