INTEGRATING OBSERVEIT WITH ARCSIGHT CEF

OBSERVEIT V6.1 AND ABOVE

Contents

1 About This Document

The purpose of this document is to provide instructions on how to integrate ObserveIT log data into the ArcSight SIEM product by using the Common Event Format (CEF) open log management standard.

Note: This document is relevant for ObserveIT version 6.1 and above.

2 Overview

Integration with the ArcSight SIEM product enables the export of ObserveIT log data to ArcSight CEF format. All log files from ObserveIT user activities, DBA activity, activity alerts, system events, In-App Elements, and auditing activities, can be exported and integrated in the SIEM monitoring software. SIEM integration parses these files based upon text strings that appear inside the log.

All ObserveIT log data is stored in one file; by default, "`Observeit_activity_log.cef`". The ObserveIT data log file must be located in a library to which the ObserveIT Notification Service user has write permissions. By default, the log file location is "`C:\Program Files(x86)\ObserveIT\NotificationService\LogFiles\ArcSight`".

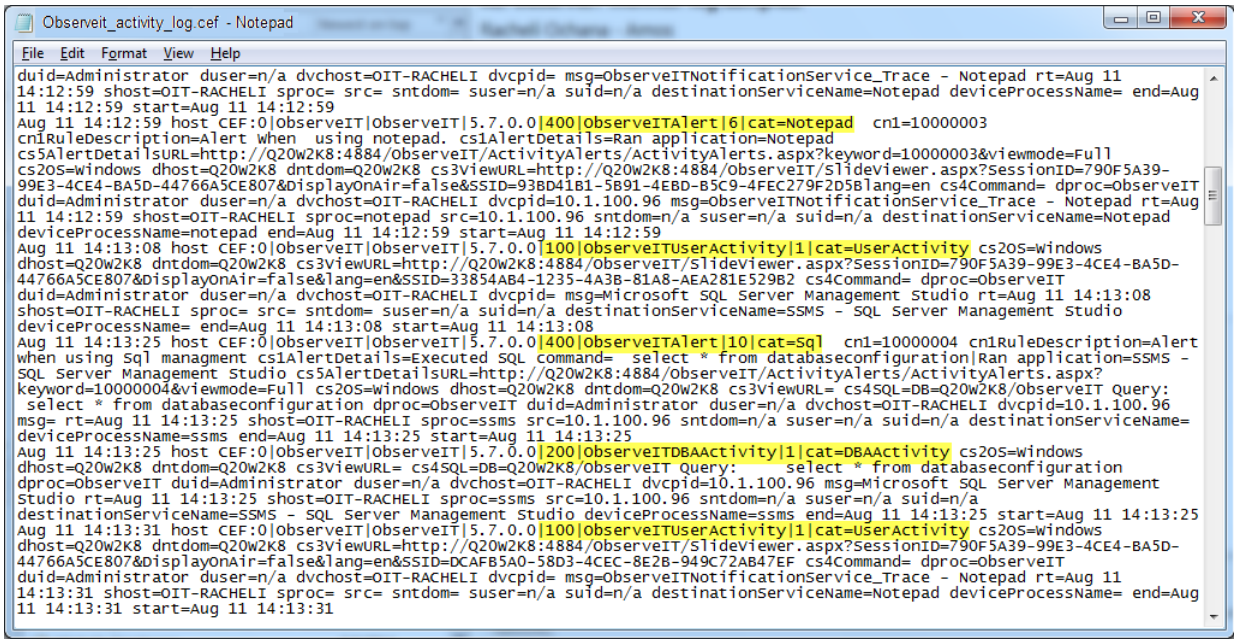
Note: The user account used by the ObserveIT Notification Service must have read and write permissions for the path. If the user account does not have sufficient permissions to create the directory or write to the log file, a system event is generated. In addition, the log file size is limited to a predefined size; if the file size exceeds the maximum defined size, a system event will be generated.

Typical log data that can be exported to ArcSight CEF format for the different data types includes:

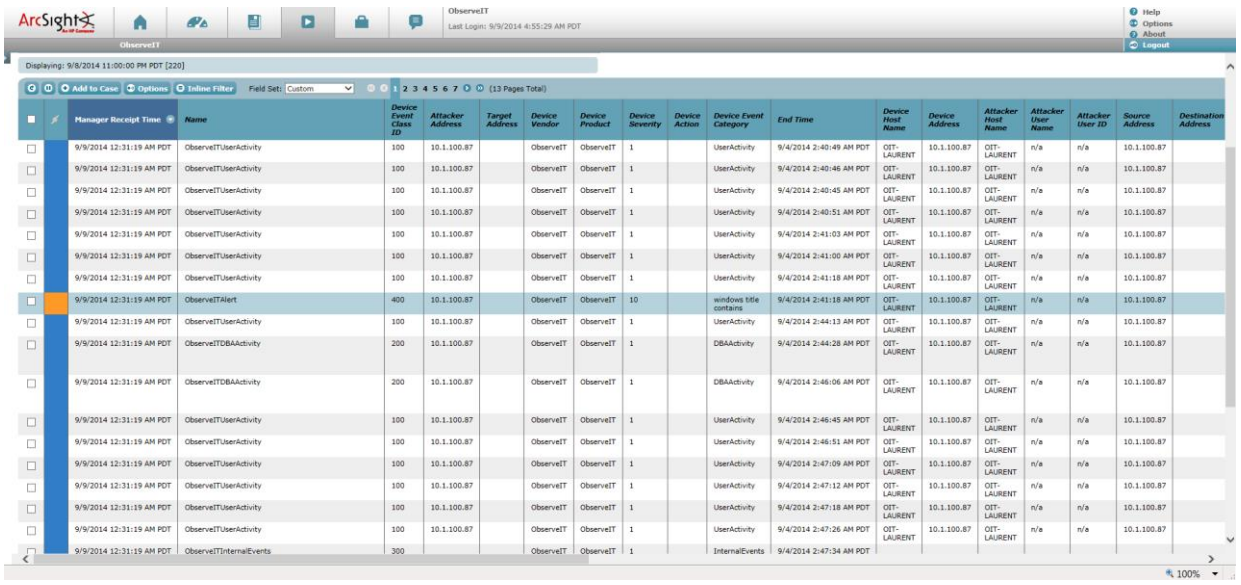
Data Type	Log Data
User Activity	OS, Server Name, Domain Name, Viewer URL, Command (Unix only), Login Name, User Name, Client Name, Client Address, Window Title, Process Name, User Authentication, Application Name
DBA Activity	OS, Server Name, Domain Name, Viewer URL, Login Name, User Name, SQL Query, DB User Name, Client Name, Client Address, Window Title, Process Name, User Authentication, Application Name
Alerts Activity	Severity, Rule Name, Alert ID, Alert Details, Alert Details URL, Viewer URL, Session identifiers according to the alert type: • Activity alert - all user activity identifiers • DBA alert - all DBA activity identifiers
System Events	Server Name, Domain Name, Event code, Event Description, Event Parameters, Source, Category, Login Name, User Name, User Authentication, Process Name
In-App Elements	StartTime (ScreenshotTime), SessionDay, SessionID, ScreenshotID, InAppElementName, InAppElementValue, InteractionIsClicked, InteractionIsDisplayed, IsMetadataOnly
Audit Session Activity	Audit Time, Console User, Domain Name, Client Address, Session ID
Audit Login Activity	Audit Time, Login Status, Login Status Description, Console User, Domain Name, Client Address
Audit Configuration Changes Activity	Audit Time, Console User, Domain Name, Client Address, Area, Item, Action, Configuration Property Name, Configuration Action, New Value

Note: For details of the ObserveIT to ArcSight field mapping definitions for each data type, see **Mapping ObserveIT Data to the ArcSight Data Fields.**

The following is an example of the contents of a CEF log file. The highlighted content shows the CEF header definitions for the user activity, DBA activity, and alerts activity data types.



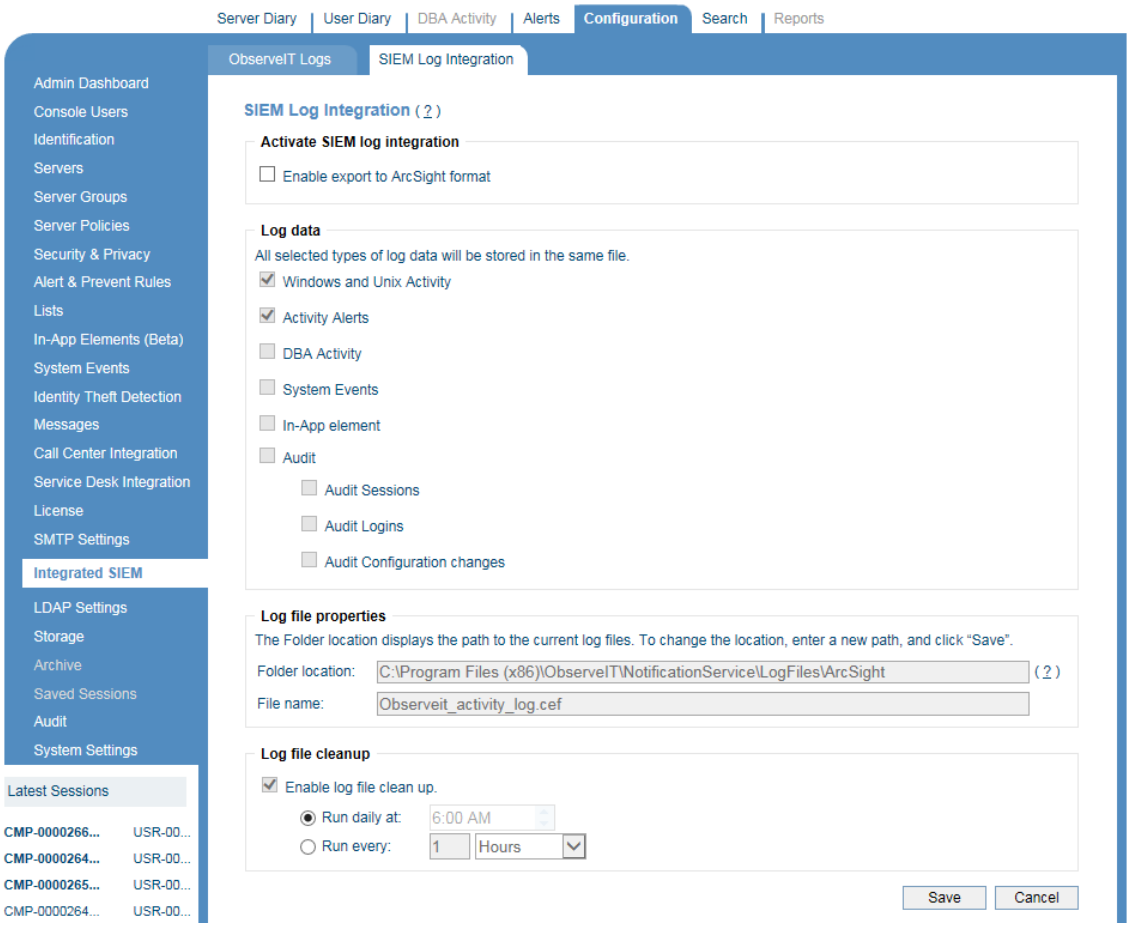
The following screenshot provides an example of how ObserveIT user activity and alert data is incorporated within ArcSight.



3 Configuring ObserveIT SIEM Integration

➢ To configure ObserveIT SIEM log integration

1 In the ObserveIT Web Management Console, open the "**SIEM Log Integration**" tab by selecting "**Configuration**" > "**Integrated SIEM**" > "**SIEM Log Integration**".



2 Activate SIEM log integration by selecting the check box "**Enable export to ArcSight format**".

3 In the "**Log data**" section, select at least one of the following data types for monitoring:

- Windows and Unix Activity (selected by default)
- Activity Alerts (selected by default)
- DBA Activity
- System Events
- In-App Elements
- Audit
- Audit Sessions
- Audit Logins
- Audit Configuration Changes

4 Under "**Log file properties**":

a. In the "**Folder location**" field, accept the default log file location: "`C:\Program Files(x86)\ObserveIT\NotificationService\LogFiles\ArcSight`" or specify a new path to the monitor log files.
When changing the default log folder location, new session data will be stored in the new path; existing data will remain in the old location.

b. In the "**File name**" field, accept the default log file name "`Observeit_activity_log.cef`" or specify a new one.

5 Under "**Log file cleanup**":

a. Select the check box to enable log file cleanup.

Note: If you deselect the check box, make sure that you have enough disk space to store the logs.

b. If log file cleanup is selected, schedule the frequency for clearing the log file:

- Select **Run daily at**, and specify the required time of day for the daily cleanup.

-Or-

- Select **Run every**, and specify the required number of days, hours, or minutes after which the log file cleanup process will take place.

6 Click "**Save**" to save your configuration.

After a few minutes, the log file will be generated. A new log file will be created according to the scheduled cleanup frequency.

Note: If required, you can configure advanced log settings by changing specific log parameters in the ObserveIT Notification Service configuration file, as described in the next section.

3.1 Configuring Advanced Log Settings

If required, you can change the configuration of specific log file parameters in the ObserveIT Notification Service configuration file.

➢ **To configure advanced log settings**

1 Open the `ObserveIT.WinService.exe.config` configuration file under `C:\Program Files (x86)\ObserveIT\NotificationService\`.

2 Locate the `<ArcSightSettingsGroup>` section in the configuration file.

```
<ArcSightSettingsGroup>
  <ArcSightSettings>
    <!--Supported Size Units:GB,MB,KB,Bytes -->
    <add key="MaximumFileSize" value="256GB" />
    <add key="HideEmptyandDuplicateFields" value="True"/>
    <add key="ShowSyslogHeader" value="True"/>
    <add key="ExposeLabeledNames" value="True"/>
    <!-- How many MINUTES to leave in log file in Cleanup process, default 60 minutes-->
    <add key="RemainingLogTime" value="60"/>
    <add key="SelectedDateFormat" value="MMM dd HH:mm:ss"/>
    <!--Supported Date Formats -->
    <!--add key="SelectedDateFormat" value="MMM dd HH:mm:ss" -->
    <!--add key="SelectedDateFormat" value="MMM dd HH:mm:ss.FFF zzz"  -->
    <!--add key="SelectedDateFormat" value="MMM dd HH:mm:ss.FFF" -->
    <!--add key="SelectedDateFormat" value="MMM dd HH:mm:ss zzz" -->
    <!--add key="SelectedDateFormat" value="MMM dd yyyy HH:mm:ss" -->
    <!--add key="SelectedDateFormat" value="MMM dd yyyy HH:mm:ss.FFF zzz" -->
    <!--add key="SelectedDateFormat" value="MMM dd yyyy HH:mm:ss.FFF" -->
    <!--add key="SelectedDateFormat" value="MMM dd yyyy HH:mm:ss zzz" -->
  </ArcSightSettings>
</ArcSightSettingsGroup>
```

3 You can change the default values of any of the following parameters:

- **MaximumFileSize**: Specify the maximum size of the "`Observeit_activity_log.cef`" file. If the file size reaches or exceeds the maximum defined size, a system event will be generated. Default size is 256 GB.

- **HideEmptyandDuplicateFields**: By default, this value is true which means that empty ("null") CEF field entries will be removed, as well as field names that are duplicated (for example, they are not relevant to other than the current data type). Change the value to "False" if you want all fields to be displayed, including empty and duplicated ones.
- **ShowSyslogHeader**: The syslog header is displayed by default. If you don't want to display the syslog header, change the value to "False".
- **ExposeLabeledNames**: By default, names of CS CEF files are exposed (e.g., "CS1AlertDetails"). You can change the value to "False" in order not to expose the file names (i.e., CS1").
- **RemainingLogTime**: Specify (in minutes) how much of the log should remain in the log file after the cleanup process.
- **SelectedDateFormat**: Replace the value with a new date in the specified format.

4 Save and exit the `ObserveIT.WinService.exe.config` configuration file.
5 Restart the ObserveIT Notification Service.

Note: Changes will only take effect after you restart the Notification Service.

4 Integrating the ObserveIT Log File into ArcSight CEF

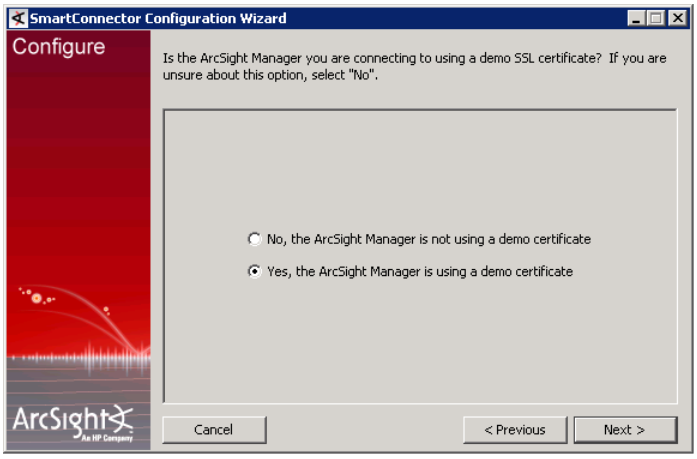
Log type data from all ObserveIT user activities, DBA activity, auditing activity, activity alerts and system events, is exported to ArcSight CEF format for integration in the SIEM monitoring software. All the selected log type data is stored in one file; by default, "`Observeit_activity_log.cef`".

The ObserveIT CEF log file is sent to the **ArcSight SmartConnector** for integration in the SIEM monitoring software.

➢ **To integrate the ObserveIT log file into the ArcSight SmartConnector**

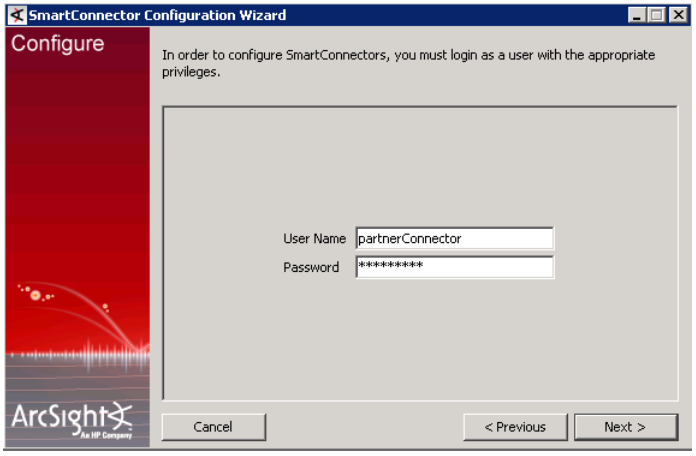
1 In the ArcSight portal, open the **ArcSight Smart Connector Configuration Wizard**.
2 Select **ArcSight Manager** as the destination type for the **SmartConnector**.

3 Specify whether or not the ArcSight Manager is using a demo SSL certificate.
If you are using a demo certificate, you must first copy the certificate file "cacerts" (approx. 94 KB) and place the attached file in the <arcsight_home>/current/jre/lib/security/ folder.

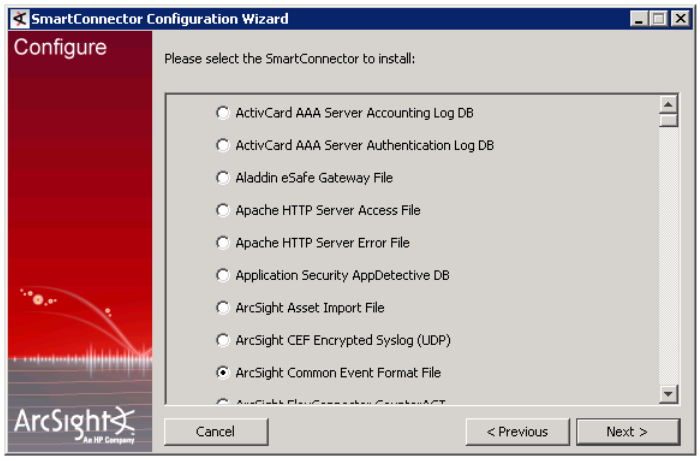


4 Specify the ArcSight Manager information in the following screen.

5. Login as a user with the appropriate privileges.

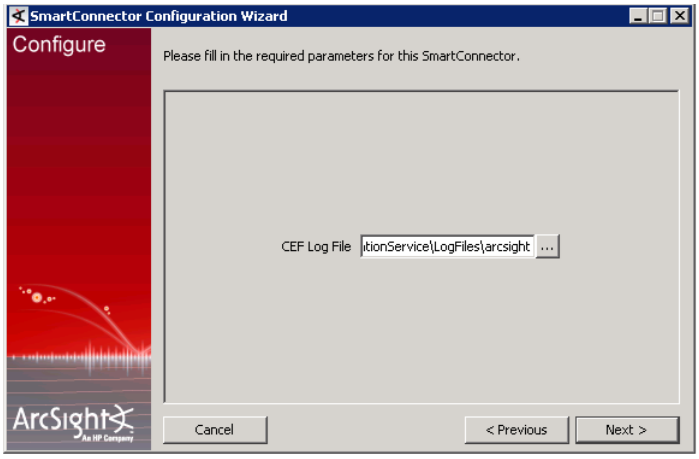


6. In the following screen, select "ArcSight Common Event Format File" as the SmartConnector to be installed.

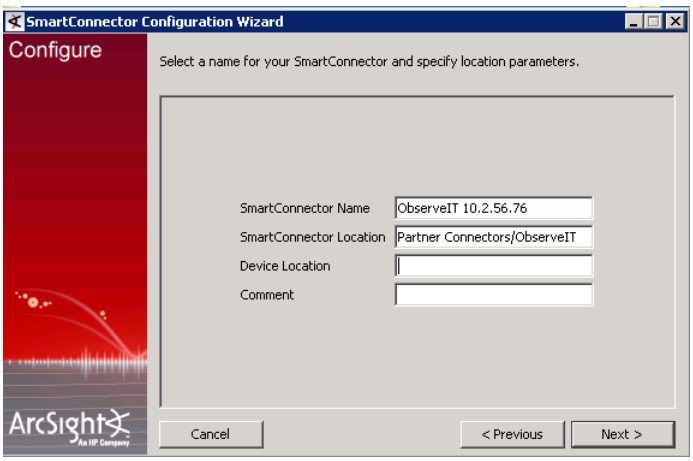


7 In the following screen, specify the log file location and CEF log file name, as configured in the ObserveIT SIEM log integration screen:
"`C:\Program Files(x86)\ObserveIT\NotificationService\LogFiles\ArcSight\Observeit_activity_log.cef`".

Note: You can change the default location and file name, if required.



8 Configure a name for the SmartConnector location and specify location parameters.



After completing the steps of the Smartconnector Configuration Wizard, the ObserveIT log file will be integrated into ArcSight.

5 Mapping ObserveIT Data to the ArcSight Data Fields

The **ArcSight SmartConnector** uploads the data from the CEF log file and maps it to the ArcSight data fields. This section describes how the ObserveIT data fields are mapped to the ArcSight data field definitions for each type of data.
For a description of the ObserveIT data fields, see the ObserveIT Log Data Dictionary of Terms.

Note: The data fields that are displayed may depend on the configuration of specific log file parameters in the ObserveIT Notification Service configuration file, as described in *Configuring Advanced Log Settings*.

5.1 ArcSight CEF Header Definitions

In the ArcSight CEF header, a signature ID unique identifier is used for each ObserveIT data type:

- User activity = 100
- DBA activity = 200
- System events = 300
- Alerts activity = 400
- Auditing activity = 500
- In-App Elements = 600

5.2 *Mapping User Activity Output*

The following table lists the mappings to the ArcSight CEF data field definitions from the ObserveIT data fields for the user activity data type:

Observe IT Data	CEF Log Definition
date	header
" host CEF:0|ObserveIT|ObserveIT| Version|100|ObserveITUserActivity|1|cat=UserActivity"	header
OS	cs2OS
Server Name	dhost
Domain Name	dntdom
Viewer URL	cs3=ViewURL
Command	cs4=Command, msg
"ObserveIT"	dproc
Login Name	duid
User Name	duser, suser, suid
Client Name	dvchost, shost
Client Address	dvcpid, src
Window Title	msg
date	rt, end, start
Process Name	sproc
User Authentication	sntdom
Application Name	destinationServiceName
Process Name	deviceProcessName

Following is an example of user activity mapping data in ArcSight:

Manager Receipt Time	Name	Event Class ID	Attacker Address	Target Address	Device Vendor	Device Product	Device Severity	Device Action	Device Event Category	End Time	Device Host Name	Device Address	Attacker Host Name
9/11/2014 12:55:41 AM PDT	ObserveITUserActivity	100	10.0.0.18	10.1.100.96	ObserveIT	ObserveIT	1		UserActivity	9/11/2014 12:48:16 AM PDT	RACHELI-W7	10.0.0.18	RACHELI-W7
9/11/2014 12:55:35 AM PDT	ObserveITUserActivity	100	10.0.0.18	10.1.100.96	ObserveIT	ObserveIT	1		UserActivity	9/11/2014 12:48:13 AM PDT	RACHELI-W7	10.0.0.18	RACHELI-W7
9/11/2014 12:55:35 AM PDT	ObserveITUserActivity	100	10.0.0.18	10.1.100.96	ObserveIT	ObserveIT	1		UserActivity	9/11/2014 12:48:17 AM PDT	RACHELI-W7	10.0.0.18	RACHELI-W7

Attacker

Attacker Address:	10.0.0.18
Attacker Asset ID:	4AuCtY0gBABDVMqDDv0wNJg==
Attacker Host Name:	RACHELI-W7
Attacker Nt Domain:	n/a
Attacker Process Name:	Notepad
Attacker User ID:	n/a
Attacker User Name:	n/a
Attacker Zone:	<Resource URI="/All Zones/ArcSight System/Private Address Space Zones/RFC1918: 10.0.0.0-10.255.255.255" ID="ML8022AABABCDTFpYAT3UdQ==/>
Attacker Zone ID:	ML8022AABABCDTFpYAT3UdQ==
Attacker Zone Name:	RFC1918: 10.0.0.0-10.255.255.255
Attacker Zone URI:	/All Zones/ArcSight System/Private Address Space Zones/RFC1918: 10.0.0.0-10.255.255.255

Target

Target Address:	10.1.100.96
Target Asset ID:	4fKWWikYBABDHSg6izI0M0Q==
Target Host Name:	OIT-RACHELI
Target Nt Domain:	observeit-sys.local
Target Process Name:	ObserveIT
Target Service Name:	Notepad
Target User ID:	racheli
Target User Name:	n/a
Target Zone:	<Resource URI="/All Zones/ArcSight System/Private Address Space Zones/RFC1918: 10.0.0.0-10.255.255.255" ID="ML8022AABABCDTFpYAT3UdQ==/>
Target Zone ID:	ML8022AABABCDTFpYAT3UdQ==
Target Zone Name:	RFC1918: 10.0.0.0-10.255.255.255
Target Zone URI:	/All Zones/ArcSight System/Private Address Space Zones/RFC1918: 10.0.0.0-10.255.255.255

5.3 *Mapping DBA Activity Output*

The following table lists the mappings to the ArcSight CEF data field definitions from the ObserveIT data fields for the DBA activity data type:

Observe IT Data	CEF Log Definitions
date	header
"host CEF:0|ObserveIT|ObserveIT| Version|200|ObserveITDBAActivity|1|cat=DBAActivity"	header
OS	Cs2OS
Server Name	dhost
Domain Name	dntdom
Viewer URL	cs3=ViewURL
Command	Cs4=SQL
"ObserveIT"	dproc
Login Name	duid
UserName: UserName SQLUSER : SqlUserName	duser, suser, suid
Client Name	dvchost, shost
Client Address	dvcpid, src
Window Title	msg
date	rt, end, start
Process Name	sproc
User Authentication	sntdom
Application Name	destinationServiceName
Process Name	deviceProcessName

5.4 *Mapping Activity Alerts Output*

The following table lists the mappings to the ArcSight CEF data field definitions from the ObserveIT data fields for the activity alerts data type:

Observe IT Data	CEF Log Definitions
date	header
host CEF:0|ObserveIT|ObserveIT|Version|400|ObserveITAlert|[Alert Severity 6/8/10]|cat=Sql	header
Alert ID	cn1Alert ID
Rule name	cn1RuleDescription
Alert Rule details	cs1AlertDetails

Alert URL	Cs5AlertDetailsURL
OS	Cs2OS
Server Name	dhost
Domain Name	dntdom
Viewer URL	Cs3ViewURL
"ObserveIT"	dproc
Login Name	duid
User Name	duser, suser, suid
Client Name	dvchost, shost
Client Address	dvcpid, src
Window Title	msg
Process Name	sproc,
date	rt, end, start
User Authentication	sntdom
Application Name	destinationServiceName
Process Name	deviceProcessName
Session ID	sourceServiceName
Screenshot ID	RequestMethod
Alert Description	reason

5.5 *Mapping System Events Output*

The following table lists the mappings to the ArcSight CEF data field definitions from the ObserveIT data fields for the system events data type:

Observe IT Data	CEF Log Definitions
Event Time	header
" host CEF:0|ObserveIT|ObserveIT| Version|300| ObserveITInternalEvents|1|cat= ObserveITInternalEvents"	header
Event Category	Cs1=Event Category
Event source	Cs2=Event Source
Server Name	dhost
Domain Name	dntdom
Event Code	Cs3=EventTypeCode
Event Desc	Cs4=EventDesc, msg
Event Parameters	Cs5=EventParameters ***Note: The format of the Event Parameters field was changed. In order to avoid ArcSight formatting problems, the list of "`key=value;`" pairs was changed to "`key:value;`" pairs.***
"ObserveIT"	dproc
Login Name	duid
User Name	duser, suser, suid
date	rt, end, start
User Authentication	sntdom
Process Name	deviceProcessName

5.6 *Mapping In-App Elements Output*

The following table lists the mappings to the ArcSight CEF data field definitions from the ObserveIT data fields for the In-App Elements data type:

Observe IT Data	CEF Log Definitions
date	header
" host CEF:0|ObserveIT|ObserveIT|Version|600| ObserveITInAppElements|1|cat=InAppElements"	header
"ObserveIT"	dproc
InAppElementName	act
InAppElementText	msg
SessionDay	rt
SessionID	sourceServiceName

ScreenshotID	requestMethod
InteractionIsClicked	Cs2InteractionIsClicked
InteractionIsDisplayed	Cs3InteractionIsDisplayed
IsMetadataOnly	Cs5IsMetadataOnly
date	end, start

5.7 Mapping Audit Activity Output

5.7.1 Audit Session Activity

The following table lists the mappings to the ArcSight CEF data field definitions from the ObserveIT data fields for the audit session activity data type:

Observe IT Data	CEF Log Definition
Audit Time	header
" host CEF:0|ObserveIT|ObserveIT| Version|500|ObserveITSessionAudit|1|cat=SessionAudit"	header
LoginStatus	Cs1
LoginStatusDescription	Cs2
DomainName	dntdom
"ObserveIT"	dproc
UserName	duser
AuditTime	rt, end, start
ClientAddress	dvc

5.7.2 Audit Login Activity

The following table lists the mappings to the ArcSight CEF data field definitions from the ObserveIT data fields for the audit login activity data type:

Observe IT Data	CEF Log Definition
Audit Time	header
" host CEF:0|ObserveIT|ObserveIT| Version|500|ObserveITLoginAudit|1|cat=LoginAudit"	header
SessionId	cs1
OperatorDomainName	dntdom
"ObserveIT"	dproc
OperatorUsername	duser
AuditTime	rt, end, start
IPAddress	dvc

5.7.3 Audit Configuration Changes Activity

The following table lists the mappings to the ArcSight CEF data field definitions from the ObserveIT data fields for the audit configuration changes activity data type:

Observe IT Data	CEF Log Definition
Audit Time	header
" host CEF:0|ObserveIT|ObserveIT| Version|500|ObserveITConfigChangesAudit|1|cat=Config ChangesAudit"	header

Area (WebConsoleItem)	Cs1
Item (ConfigurationItem)	Cs2
UserDomainName	dntdom
Action (TypeOfChange)	Cs3
ConfigProprtyName (ParentConfigurationItem)	Cs4
TypeOfChangeStr	Cs5
NewValue	Cs6
Area:{0},Item:{1},Action:{2},ConfigProprtyName:{3},TypeOfChangeStr:{4},NewValue:{5}	msg
UserLoginName	suser, suid
ClientIP	dvc
AuditTime	end, start

6 ObserveIT Log Data Dictionary of Terms

Observe IT Data	Definition
date	Date and time the activity occurred: e.g., Aug 13 2014 15:25:48
OS	Operating system (e.g., Windows, Unix)
Server Name	The server on which the activity occurred: e.g., Q8-Wo8SQo8-2
Domain Name	The domain name of the user.
Viewer URL	Link to the Session Player for the recorded session. e.g., http://Q8-W08SQ08- 2:4884/ObserveIT/SlideViewer...
Command	SQL command with the following structure: "*DB=SqlDBName* *Query:SqlQueryText*" For example: *DB=10.2.56.76/ObserveIT* *Query:select sdatetime, s.sessionid, shot.ssid, s.clientname,…*
"ObserveIT"	ObserveIT
Login Name	Login name of the user who ran the session in which the activity occurred (e.g., `obsqa8.local\administrator`).
User Name	If configured, secondary identification of the user who ran the session in which the activity occurred (`obsqa8.local\administrator`).
Client Name	Name of the client computer from which the activity occurred (e.g., `OIT-JOHNS-LAP`)
Client Address	IP address of the client computer from which the activity occurred (e.g., `10.2.56.76`).
Window Title	Program Manager
date	Date and time of the activity (e.g., `Aug 13 2014 15:25:48`)
Process Name	Name of the process currently running (e.g., `iexplore`)
User Authentication	Secondary authentication user login.
Application Name	Name of the application currently running (e.g., `Windows Explorer`)
Alert ID	Unique number that identifies the alert. For example: `10000001`
Rule Name	A unique name that describes the alert rule (e.g., Alert when using SQL management.
Alert Rule Details	What the user did to trigger the alert. For example: "*Executed SQL command=Select "from databaseconfiguration| Ran application=SSMS - SQL Server Management Studio*"
Alert URL	Clicking the Alert ID in the link opens the Alert Activities UI page to show the selected alert, in "Show: Full Details" mode.
Event Category	The category to which an event belongs (e.g., Login, Health Check).

Event Code	A unique code that identifies an event.
Event Source	Source from which an event is triggered (e.g., Identity theft, Notification Service).
Event Desc	Description of an event (e.g., Notification Service stopped).
Event Parameters	Additional information related to an event (e.g., the name of the database).
SessionDay	The date that the In-App element was captured.
InAppElementName	Name of the In-App element captured by the Marking Tool.
InAppElementValue	Value of the displayed element (e.g., Export Button).
InteractionIsClicked	The element interaction type is "Clicked".
InteractionIsDisplayed	The element interaction type is "Displayed".
IsMetadataOnly	The In-App element has metadata only.
AuditTime	The time that an audit entry was created.
ConsoleUser	Console User that accessed the Web Console.
LoginStatus	Indication of whether the user login was successful or failed.
LoginStatusDescription	Description of the reason for a failed login.
Area	Area in the Web Console in which configuration changes were made (e.g., Server Policy, Licensing, Session Privacy, Application Server).
Item	Item in the Area of the Web Console on which the configuration was changed (e.g., LDAP Target Domain, Default Windows-based Policy).
Action	Action that was performed on the configured item (e.g., Changed, Removed, Added).
ConfigPropertyName	The specific property of a configuration Item that was changed. For example, "System Policy – Enabled keylogging" refers to the property of a specified server policy.
ConfigAction	The action that was performed on the configuration property item (e.g., Changed to)
NewValue	New value that was given to a changed configuration property item (e.g., Disabled).