opentext™

ArcSight User Behavior Monitoring

Software Version: 24.3

Solutions Guide

Legal Notices

Open Text Corporation

275 Frank Tompa Drive, Waterloo, Ontario, Canada, N2L 0A1

Copyright Notice

Trademark Notices

Support

Contact Information

Phone	A list of phone numbers is available on the Technical Support Page: https://softwaresupport.softwaregrp.com/support-contact-information
Support Web Site	https://softwaresupport.softwaregrp.com/
ArcSight Product Documentation	https://www.microfocus.com/documentation/arcsight/

About this PDF Version of Online Help

This document is a PDF version of the online help. This PDF file is provided so you can easily print multiple topics from the help information or read the online help in PDF format. Because this content was originally created to be viewed as online help in a web browser, some topics may not be formatted properly. Some interactive topics may not be present in this PDF version. Those topics can be successfully printed from within the online help.

Contents

Chapter 1: ArcSight User Behavior Monitoring Solution Overview

In the past, IT security professionals were predominantly concerned with protecting their assets by keeping unauthorized individuals out of their networks. Today, they must continue to protect their assets while granting access to a wide range of different individuals. Full-time and part-time employees, contractors, partners, and customers all require varying levels of access to resources. Managing the proper level of access for all individuals is challenging even in the simplest network environments.

Identity Management Systems provide role-based access controls (RBAC) to protect assets. In Identity Management Systems, access to an asset by an individual user can be provisioned based on the following factors:

- The business or IT role of the user (for example: the dba role)
- The user's organizational unit (for example: Engineering department)
- The user's employee type (for example: full time)
- Specific access requirements of the user

The ArcSight User Behavior Monitoring (UBM) solution provides the ability to correlate identity information maintained in your Identity Management System with the events generated in your network. This ability means that those network events can be enriched with contextual user information, such as:

- Who is the person that caused the event to be generated?
- What is their business or IT role, or other attributes such as Department and Employee Type?
- Should they have had the right to perform that activity?

What Use Cases are Provided?

The UBM solution resources are grouped together in the ESM Console using use case resources. A use case resource provides a way to group a set of resources that help address a specific security issue or business requirement. For more information, see ArcSight User Behavior Monitoring Use Cases.

The UBM solution provides the use cases listed in the following table.

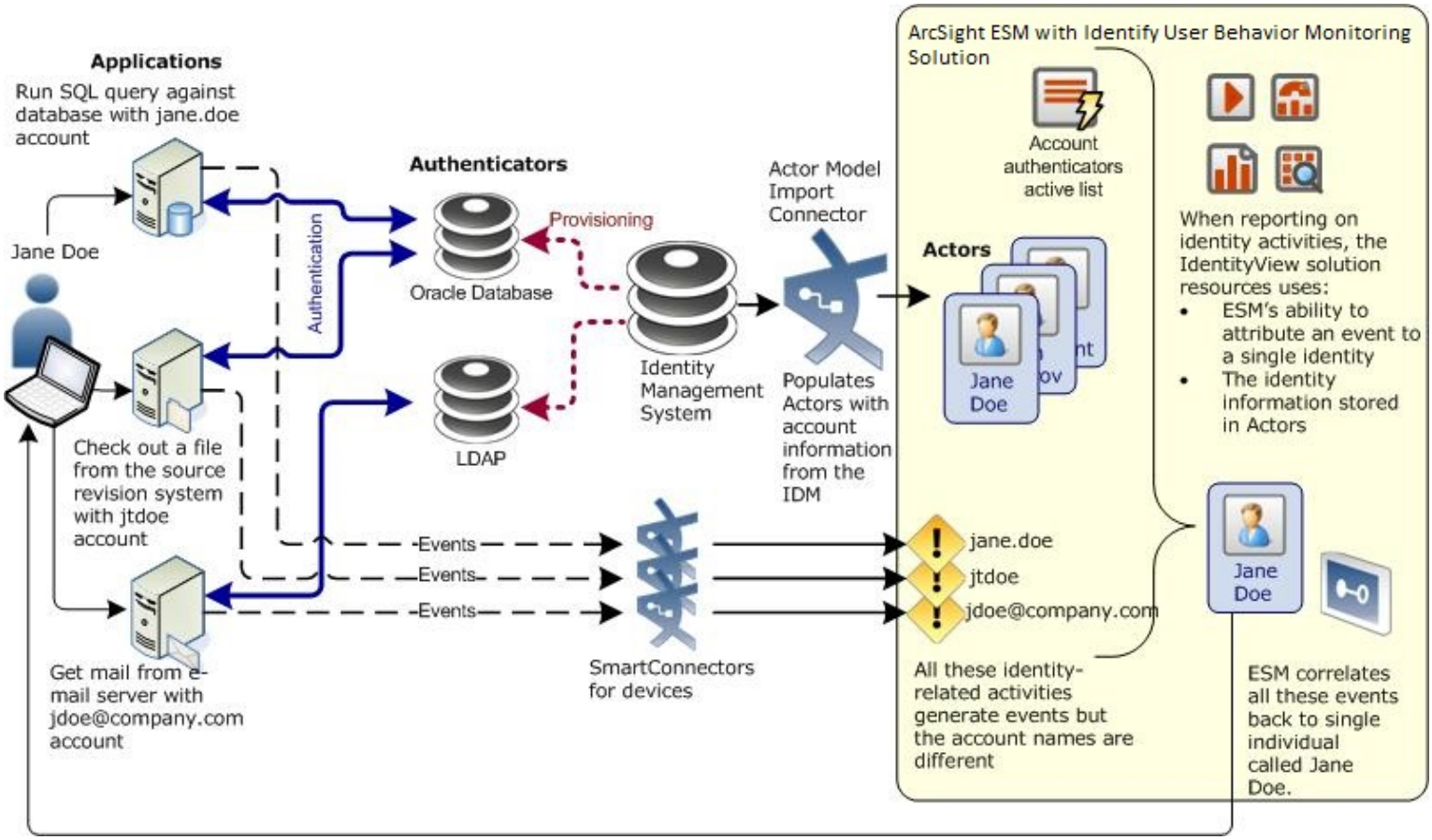
Use Case Name	Use Case Description
Actor Attribution by IP Address Use Case	The Actor Attribution by IP Address use case associates IP addresses to actors, and allows events from IP addresses to be attributed to the logged in actor, even if no username is present in the event.
Actor Management Use Case	The Actor Management use case contains resources designed to show analysts the status of actor resources in ESM. The number of actors, roles, and account IDs monitored can be identified with this use case. In addition, analysts can monitor changes to actor resources, and identify the use of rogue accounts that cannot be tied to any actor in ESM.
Actor Threat Score Use Case	The Actor Threat Score use case provides a method for tracking the level of suspicious activity exhibited by monitored users. Analysts are notified when an actor's suspicious activity exceeds configurable levels. Actors with high threat scores are monitored at a higher level of scrutiny.
Privileged User Monitoring Use Case	The Privileged User Monitoring use case monitors the usage and authorization of privileged accounts.
Shared Accounts Use Case	The Shared Accounts use case reports on the usage of accounts that might be in use by more than one individual. The use case can detect when anyone uses an existing known shared account, as well as detect the use of any account by more than one individual.
Suspicious Activity Use Case	The Suspicious Activity use case provides resources that can be used to discover and analyze suspicious activity occurring on your network. When triggered, the suspicious activity rules can contribute to the resources of the Actor Threat Score Use Case.
User Activity Monitoring Use Case	The User Activity Monitoring use case contains resources designed to enable analysts to monitor the activity of users on the network. Many resources break down activity by actors' employee type, department, or other attributes.

How Does the Solution Work?

The UBM solution is driven by data provided from the following two sources:

- Event data from devices reporting on user account activities such as running a SQL query, checking out a file from a source revision system, and getting email from an email server.
- Identity data typically provided by an Identity Management System as shown in the graphic below. This identity data is stored in ESM as actors which might represent a single individual.

Overview of the Solution Architecture



Note:Provisioning: Accounts, Roles, and Access Permissions are assigned by the Identity Management System.
Authentication: The process of validating credentials from an individual against the information stored in the Authenticator.

Actors

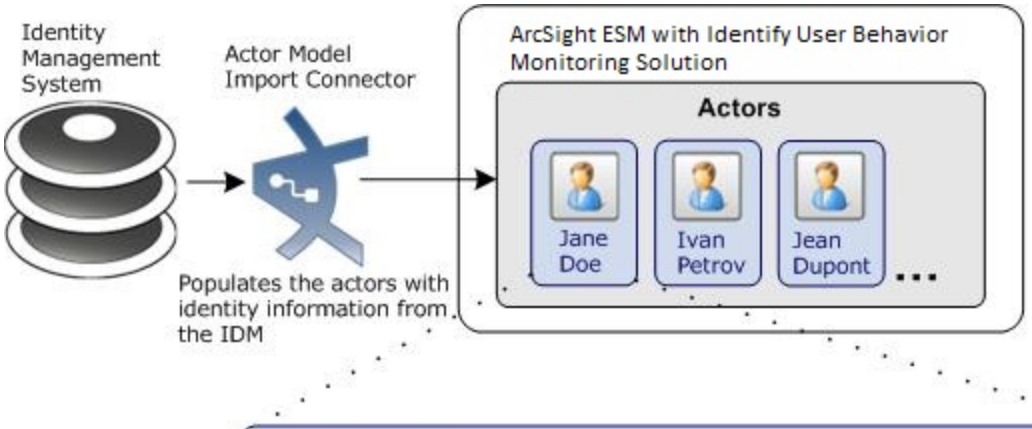
An *actor* is an ESM resource that stores identity information and most commonly represents a single individual. For example, the Jane Doe actor contains identity information about the individual called Jane Doe. The UBM solution leverages ESM's actors resource for reporting and correlation.

SmartConnectorfor Actor Model Import

As shown in the Overview diagram above, actors are typically populated in ESM from an Identity Management System using a SmartConnector for Actor Model Import. These actors are populated dynamically which means as the identity data changes in the Identity Management System, the corresponding data in the actors are automatically

updated. For example, if Jane Doe's department changes in the Identity Management System, this change is reflected in the Department attribute of the Jane Doe actor. Details about the identities such as Employee Type, Department, and Email Address are stored as actor attributes as shown in the following diagram. In addition, a Universally Unique Identifier (UUID) for the individual, which is assigned by the Identity Management System, is stored in the UUID attribute.

Populating the Actor Model from an Identity Management System



Actor Attributes

Attributes	Value
UUID	347839
First Name	Jane
Last Name	Doe
Employee Type	full time exempt
Status	active
Department	Systems Operations
Manager	Jean Dupont
Email Address	jdoe@company.com
...	...

Account Attributes

Authenticator	Account-id
Active Directory: company.com	jane doe
Active Directory: company.com	jtdoe
Active Directory: company.com	CN=Jane Doe,OU=Eng,DC=company,DC=COM

Role Attributes

Role Name	Resource Name	Role Type
Administrator	Security Software	Global Security Group

Actor Attribution

The UBM solution uses the data stored in actors and the identity correlation features of ArcSight ESM to determine the unique identity (individual) that is responsible for a set of events.

As shown on the left side above, the individual named Jane Doe uses different accounts to access assets on the network:

- Uses the jane.doe account to run a SQL query against a database.
- Uses the jtdoe account to check out a file from a source revision system.
- Uses the jdoe@company.com account to get email from an email server.

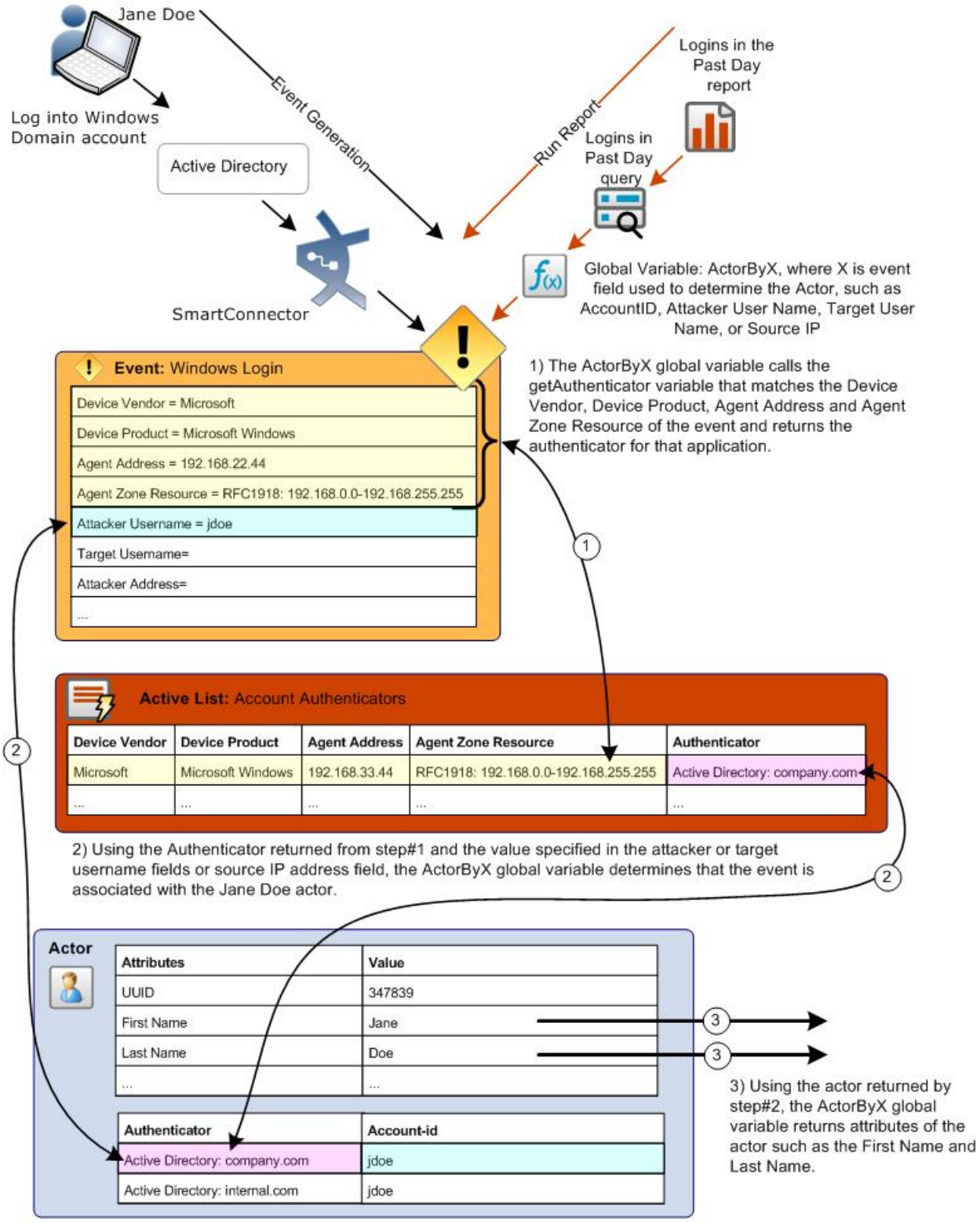
Using the actor model, ESM is able to tie all these user accounts to a single individual, or actor.

Each individual in the environment is associated with an actor in ESM. If Jane Doe accesses an email server using the account called jdoe@company.com and then accesses a database using the database account called jane.doe, ESM can correlate these two activities as originating from a single individual called Jane Doe. The UBM solution resources use this ability to correlate events to an identity and the actor attributes stored in actors to report on identity activity—a process called actor attribution. The actor attribution process is shown in the diagram below. For example, the Actor Changes report shows a count of successful logins by privileged users with the specified roles.

The UBM solution provides additional actor attribution facilities. In some cases, actor attribution cannot be performed due to a lack of identity information stored in the event. For these cases, the UBM solution attempts to identify the actor associated with the event by correlating the source IP address stored in the event with the IP address of a computer used by an actor. For more information, see Actor Attribution by IP Address Use Case.

The Account Authentication List active list is used to uniquely qualify account IDs imported from multiple authentication systems and seen in events. This list provides a way to correlate an account ID to the correct actor as shown.

Actor Attribution in UBM


Jane Doe
Log into Windows Domain account
Event Generation
Active Directory
SmartConnector
Logins in the Past Day report
Run Report
Logins in Past Day query
Global Variable: ActorByX, where X is event field used to determine the Actor, such as AccountID, Attacker User Name, Target User Name, or Source IP
Event: Windows Login
Device Vendor = Microsoft
Device Product = Microsoft Windows
Agent Address = 192.168.22.44
Agent Zone Resource = RFC1918: 192.168.0.0-192.168.255.255
Attacker Username = jdoe
Target Username=
Attacker Address=
...
1) The ActorByX global variable calls the getAuthenticator variable that matches the Device Vendor, Device Product, Agent Address and Agent Zone Resource of the event and returns the authenticator for that application.
1
Active List: Account Authenticators
Device Vendor | Device Product | Agent Address | Agent Zone Resource | Authenticator
Microsoft | Microsoft Windows | 192.168.33.44 | RFC1918: 192.168.0.0-192.168.255.255 | Active Directory: company.com
... | ... | ... | ... | ...
2) Using the Authenticator returned from step#1 and the value specified in the attacker or target username fields or source IP address field, the ActorByX global variable determines that the event is associated with the Jane Doe actor.
2
2
Actor
Attributes | Value
UUID | 347839
First Name | Jane
Last Name | Doe
...
3
3
3) Using the actor returned by step#2, the ActorByX global variable returns attributes of the actor such as the First Name and Last Name.
Authenticator | Account-id
Active Directory: company.com | jdoe
Active Directory: internal.com | jdoe
4) The IdentityView resources use the actor attribute information to report on the activities of individuals as shown represented by the orange arrows above.

For more information, see the ArcSight Console User's Guide.

Using actors and the unique identifier specified in the Identity Management System, the UBM solution can track suspicious behavior of an individual. For more information, see "Tracking Suspicious Activity By Actor Threat Score" on page 10.

Using the same unique identifier and the identity attributes stored in actors, the UBM solution can get more information about Jane Doe such as her current status, department, employee type, manager, and full name. For example, using Jane Doe's Unique ID of 347839, the UBM solution can return Jane Doe's employee type by looking up the value in the Employee Type attribute for the actor with a UUID of 347839.

Note: For more information about actors, including the maximum number of actors supported, see the ArcSight Console User's Guide.

Global Variables

In addition, the UBM solution leverages the UBM global variable resource, which makes it possible to define a variable once, then re-use it in multiple places wherever conditions can be expressed (active channels, rules, filters, data monitors, and queries), and wherever fields can be selected (CCE, field sets). Global variables are centralized and reusable, which makes them an essential building block for user correlation in the actors feature. For more information, see the ArcSight Console User's Guide.

Using global variables provided with ESM standard content and the UBM solution, identity data stored in actors can be cross-referenced dynamically during run-time by UBM solution resources that use conditions, such as filters, rules, and reports. Global variables are also used to determine the individual who initiated the activity that caused the base event—a process called actor attribution.

The above figure also shows how global variables are used in actor attribution. For a list of the global variables used for actor attribution, see the table below. For a list of all the variables included with UBM, see ArcSight User Behavior Monitoring Resources By Type.

Actor Attribution Global Variables

Global Variable	Description	URI
ActorByAccount*	This global variable maps the account information in an event with an actor. The account information consists of the device vendor and product, and information derived from the attacker or target name, with preference to the target user name.	ArcSight Solutions/UBM/Core Variables/
ActorByAttackerUserName*	This variable maps the account information in an event with an actor. The account information consists of the device vendor and product, connector address and zone, and information derived from the attacker user name.	ArcSight Solutions/UBM/Core Variables/
ActorByCustomFields*	This variable attempts to retrieve actor information from events where the authenticator information is maintained in device custom strings. It works similarly to the ActorByAccountID variable, but maps Device Custom String 1 to the vendor field, Device Custom String 2 to the product field, and Device Custom String 3 should hold the Account ID. If the events in your system are mapped in another manner, change the local variables customVendor, customProduct and getAccount to map to the appropriate fields in your events. Note that when you upgrade the system in the future, this filter might be overwritten and your changes lost.	ArcSight Solutions/UBM/Core Variables/
ActorByDN*	This Actor global variable looks for a DN (Distinguished Name) in Device Custom String1, and retrieves the Actor with that DN.	ArcSight Solutions/UBM/Core Variables/
ActorByIP*	This global variable returns all the information for an actor, where the event to actor attribution is done using the source IP address.	ArcSight Solutions/UBM/Actor Attribution by IP Address/
ActorByIPorAccount*	This variable attempts to attribute an actor to an event based on source IP or attacker or target user name fields (in that order).	ArcSight Solutions/UBM/Shared Accounts/

Global Variable	Description	URI
ActorByTargetUserName*	This variable maps the account information in an event with an actor. The account information consists of the device vendor and product, connector address and zone, and information derived from the target user name.	ArcSight Solutions/UBM /Core Variables/
ActorByUUID*	This global variable looks for a UUID in Device Custom String1, and retrieves the Actor with that UUID.	ArcSight Solutions/UBM /Core Variables/
AttributableActor	This global variable returns all information for an actor, where the event to actor distribution is done using either attacker or target user name fields, or the source IP address. Note: To turn lookups based on the source IP address, in the Parameters tab, do not use the actorByAccountOrSourceIP local variable to lookup the actor, use the UUID field of the ActorByAccountID global variable instead.	ArcSight Solutions/UBM /Core Variables/

* These global variables are linked from the ArcSight System global variables in All Fields/ArcSight System/Actor Variables/.

Global variables are available in the Navigator from Field Sets in the Fields & Global Variables tab.

Tracking Suspicious Activity By Actor Threat Score

The UBM solution tracks the suspicious behavior of actors using a threat score. For example, if Jane Doe's Windows account is locked out because a large number of incorrect password attempts, the threat score associated with the Jane Doe actor is set to 1. (Assuming that this is Jane Doe's first suspicious activity.) If Jane Doe tries to login into a database using a default account, the threat score associated with the Jane Doe actor is increased by 1, resulting in a combined threat score of 2. The threat score is associated with the Jane Doe actor and not just Jane Doe's Windows account. This means that the suspicious activity of all of Jane Doe's user accounts are tracked and not just the activity of Jane Doe's Windows account. For example, suspicious activity with Jane Doe's other user accounts like her database or her source revision system account are also tracked.

The rules provided in the Suspicious Activity Use Case drive the threat score of actors. The threat score of actors is monitored in the "ArcSight User Behavior Monitoring Use Cases" on page 40. For more information, see "ArcSight User Behavior Monitoring Use Cases" on page 40 and "ArcSight User Behavior Monitoring Use Cases" on page 40.

What is Done with the Processed Data?

The UBM solution uses data from the Identity Management System to provide identity context to event data from connectors. The identity context can be utilized in the following ways:

- The identity context can be presented to the solution audience in the form of dashboards, reports, and active channels. For example, reports can be generated to retrieve event data for all individuals in a specific department.
- Rules can use identity context to determine whether particular activity constitutes a violation. For example, contractors might not be permitted to log in to certain systems after hours. Contextual identity information is required to determine that the after hours activity was performed by a contractor.

For a listing of the UBM solution resources by use case, see the individual use case description in "ArcSight User Behavior Monitoring Use Cases" on page 40. For a list of all the UBM resources by type, see ArcSight User Behavior Monitoring Resources By Type.

How is Pattern Discovery Used?

The UBM solution can utilize ArcSight's advanced pattern detection engine to identify patterns of activity in the transaction data. The pattern engine analyzes data that has been collected and presents patterns of activity that have occurred together. Pattern Discovery profiles can be configured to look for patterns between any of the transaction attributes such as Event Name, Event Type, Source Country, or IP address. For example, a Pattern Discovery profile can look for patterns in payment activity, activity from particular countries, or account access. Once a pattern is identified, it can be saved by analysts and marked as a common pattern, or as a potentially fraudulent one. If the pattern identified is potentially fraudulent, a rule can be automatically created to detect further instances of the pattern in real-time using the correlation engine. Pattern Discovery finds patterns using advanced data mining techniques by leveraging Graph Theory Algorithms, AI, and machine learning capabilities, such as intelligent pattern recognition, predictive analytics, and statistical analysis. The correlation engine detects these patterns of activity in real-time.

The UBM solution includes predefined Pattern Discovery profiles that can be used to look for specific patterns in transaction data. Administrators can also create their own Pattern Discovery profiles if desired. Using Pattern Discovery profiles, the Pattern Discovery engine can discover patterns in your event data that you consider to be normal. Part of the Pattern Discovery life cycle is to establish a baseline of normal activity, so that unusual patterns that should be investigated stand out.

For the list of predefined Pattern Discovery profiles included with the UBM solution, see ArcSight User Behavior Monitoring Resources By Type.

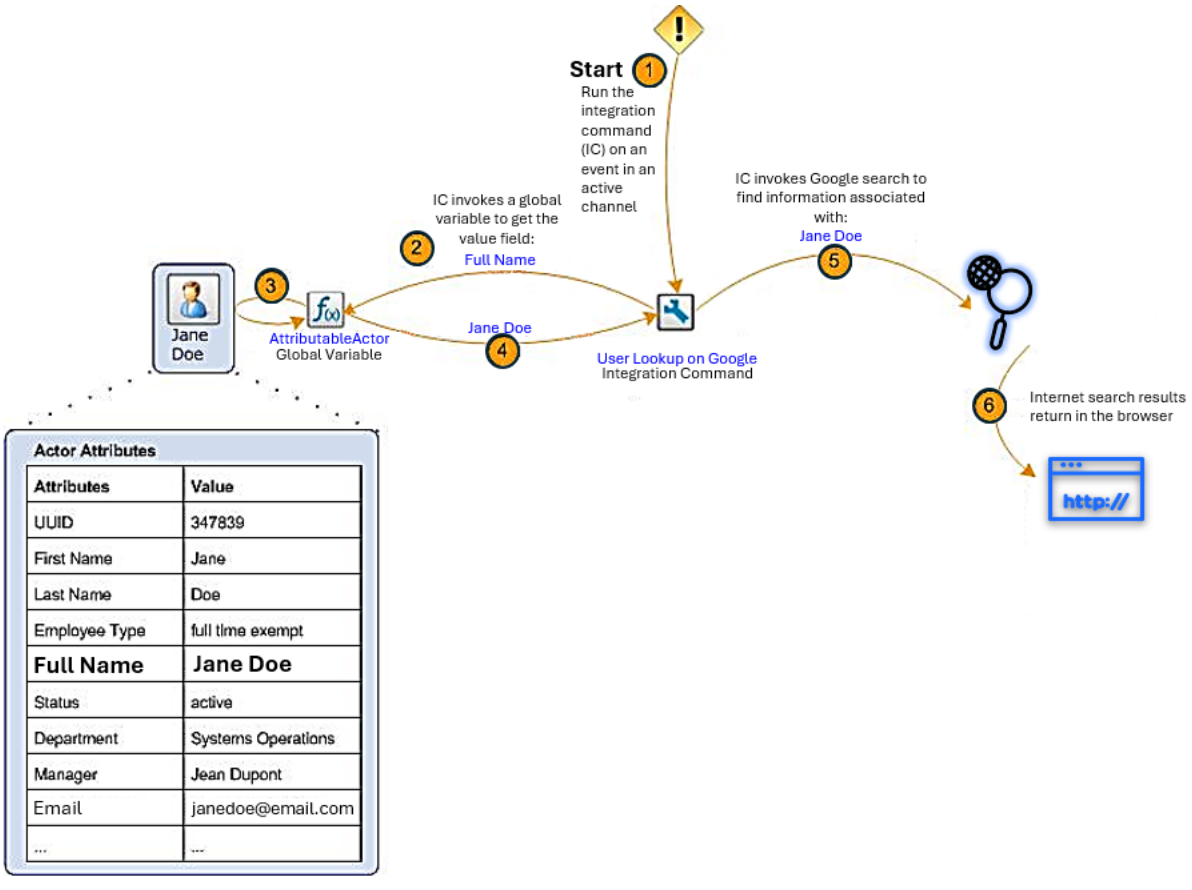
Note: The Pattern Discovery profiles included with the UBM solution can only be utilized if your ESM is licensed for Pattern Discovery.

What Integration Commands are Provided?

The UBM solution provides integration commands that can be invoked from the ESM Console and run on external web applications and ArcSight Loggers. From the ESM Console, you select an event in an active channel to investigate by running an integration command.

For example, when an integration command is run on an event in an active channel, identity data derived from the selected ESM event is processed by a UBM global variable and the result is passed into the integration command as a parameter; see steps one through three in the workflow below. The global variable attempts to attribute the event to an actor and returns the specified information for that actor; as shown by step four. Next the integration command prompts the user, asking if they want to invoke a Google search for more information associated with the actor's returned information (step 5). That search's results are then returned to the user in-browser.

Integration Command Workflow



The UBM solution integration commands are grouped in the following sections:

- "External User Lookup Integration Commands" below
- "Logger Integration Commands" below

The integration commands provided by UBM are also listed in ArcSight User Behavior Monitoring Resources By Type. For more information, see the ArcSight Console User's Guide. For more information about configuring and running the UBM solution integration commands, targets, and configurations, see "Solution Installation, Upgrade, and Configuration" on page 15.

Note: The UBM integration commands only support investigating events listed in an active channel.

External User Lookup Integration Commands

The UBM user lookup commands invoke external web applications with identity information derived from an ESM event. The UBM solution provides the following user lookup integration commands:

- **User Lookup by Actor Full Name**—This integration command gets details about the enterprise user that is associated with the event by querying a web application. The full name of the actor attributed to the event is passed into the web application as a URL parameter. NOTE: Specify parameters or modify the URL to reflect your environment.
- **User Lookup by Event User Name**—This integration command gets details about the enterprise user that is associated with the event by querying a web application. The user name associated with the event is passed into the web application as a URL parameter. NOTE: Specify parameters or modify the URL to reflect your environment.
- **User Lookup on Google**—This integration command checks the internet activity of the enterprise user that is associated with the event by querying the Google search engine. The full name of the actor attributed to the event is passed to Google.

Logger Integration Commands

The UBM Logger integration commands invoke searches on the ArcSight Loggers (appliance or software) with the account IDs derived from ESM events. The UBM solution provides the following Logger integration commands:

- **Search for Events Associated with Actor Near When the Event Occurred**—This integration command determines all the account IDs associated with the actor that is attributable to the ArcSight ESM event and then searches for events with those account IDs on Logger. The search returns all the events matching the condition within the past ten minutes since the event occurred.

Integration Targets

In addition to integration commands, the UBM solution provides integration targets that store connection information about a specific destination where the command is run. These integration targets can be used by multiple integration commands and are shared by all the users on the ESM Manager. For example, the Solutions Logger integration target can store the IP address of the Logger and the credentials used to log into the Logger. The Solutions Logger integration target is used by the following integration commands: **Search for Events Associated with Actor Near When the Event Occurred** and **Search for Events Asssociated with Actor Over the Past Day**. The UBM solution provides the integration targets listed in ArcSight User Behavior Monitoring Resources By Type. You can customize the targets to reflect devices in your organization. Integration targets are shared with all users on the same ESM Manager. In addition ESM provides the ability to save parameter data at a user level.

Integration Configurations

The UBM solution also provides integration configurations that bind integration commands to a target. For example, the UBM Logger integration command binds the **Search for Events Associated with Actor Near When the Event Occurred** and **Search for Events Asssociated with Actor Over the Past Day** integration commands to the Solutions Logger target. The integration configurations provided by the UBM solution are listed in ArcSight User Behavior Monitoring Resources By Type.

Chapter 2: Solution Installation, Upgrade, and Configuration

This section contains information on installing and configuring the ArcSight User Behavior Monitoring (UBM) solution and contains the following topics:

Prepare Your Environment

For UBM 24.3 system requirements, see the ArcSight User Behavior Monitoring 24.3 Release Notes.

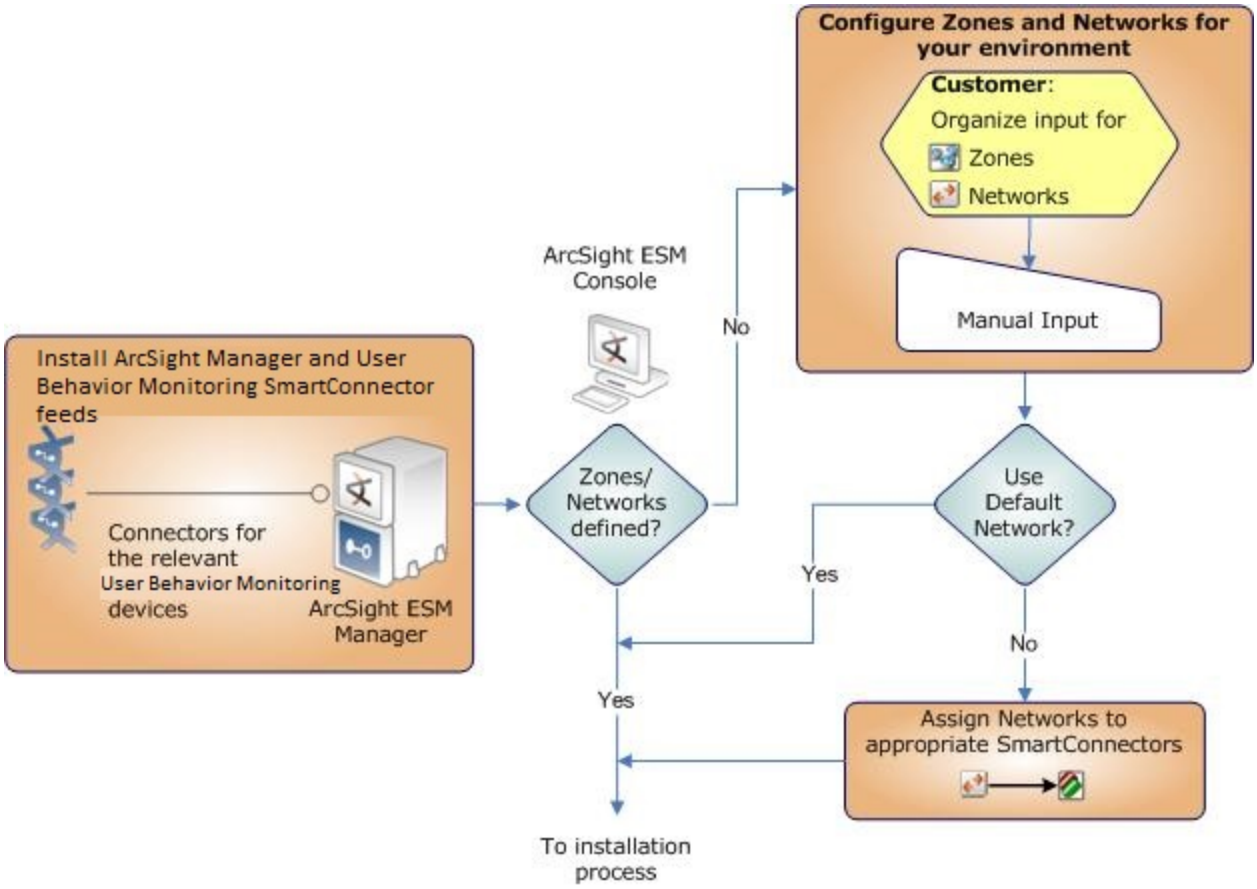
Before installing, prepare your environment for the UBM solution:

1. Install and configure the appropriate SmartConnectors for the devices found in your organization.

Note: The devices that provide events for a UBM use case are listed in the individual use case description. For more information, see "ArcSight User Behavior Monitoring Use Cases" on page 40.

2. Model your network to include UBM devices. Verify that zones and networks are defined for your organization and that networks are assigned to the connectors reporting events relative to UBM into ESM. Learn more about the ArcSight network modeling process in the ESM 101 Guide. Find instructions for how to configure zones and networks in the ArcSight Console User's Guide.

Configure Device Feeds, Zones, and Networks



Verify Your Environment

Before installing UBM, verify your ArcSight installation. The ArcSight User Behavior Monitoring 24.3 Release Notes indicate the supported versions of ArcSight ESM.

Verify that your system has the ESM Console connected to a supported ESM Manager and meets the prerequisite requirements for your operating system as detailed in the Installation and Configuration Guide for the ArcSight product.

Verify Your License

Verify that your ESM Manager is licensed for UBM. The UBM license enables the Actors feature of ESM:

Actors—The UBM solution uses the identity data stored in actors. The Actor Model Import connector populates the identity information stored in Actors on the ESM Manager. The number of Actors licensed should be equal to or greater than the number of identities imported from your Identity Management System.

For more information about licensing, see the ArcSight Console User's Guide.

Configure ArcSight ESM for a Large Number of Actors

For ArcSight ESM 7.6.5 and later, using certain Actor Model Import Connectors, UBM supports up to 500,000 actors per ESM Manager, with an average of 10 roles and 10 accounts for each actor. For information about which Actor Model Import Connectors support 500,000 actors, see the ArcSight User Behavior Monitoring Release Notes.

For organizations that have more than 300,000 actors, an ArcSight Professional Services engagement is required to assist with hardware sizing.

The following configuration is required for environments with more than 50,000 actors.

The Actor Model Import Connectors require additional memory to support 500,000 actors. For details, see the appropriate Actor Model Import Connector configuration guide.

1. SSH to the ESM Manager as the *arcsight* user.
2. Stop the ESM Manager by running the following command in the /sbin directory:

```
/sbin/service arcsight_services stop manager
```

You can check the service status by running the following command:

```
/sbin/service arcsight_services status all
```

3. Increase the maximum capacity for session lists by adding the following lines to the server.properties file in /opt/arcsight/manager/config:

```
sessionlist.max_capacity=5000000
resource.broker.cache.size.Actor=500000
persist.file.size.archive.size.max=307200
search.index.level.Actor=0
```

Note that `sessionlist.max_capacity` is set to five million, and `resource.broker.cache.size.Actor` is set to five hundred thousand.

4. Increase the memory for ESM Manager by modifying the following lines in the server.wrapper.conf file located in /opt/arcsight/manager/config, as shown below:

```
wrapper.java.initmemory=32768
wrapper.java.maxmemory=32768
```

ArcSight recommends a minimum value of 32768 MB (32 GB) to support 500,000 actors.

The initmemory and maxmemory values must be a multiple of 1024.

5. Increase the memory for the resvalidate command by editing the resvalidate.sh file in /opt/arcsight/manager/bin/scripts and change this:

```
ARCSIGHT_JVM_OPTIONS="-Xms2048m -Xmx4096m -XX:+HeapDumpOnOutOfMemoryError"
```

to this:

```
ARCSIGHT_JVM_OPTIONS="-Xms8192m -Xmx16384m -XX:+HeapDumpOnOutOfMemoryError"
```

Even after increasing the memory, only use the resvalidate command when the ESM Manager is not running.

6. Increase the memory for indexing by editing the searchindex.sh file located in /opt/arcsight/manager/bin/scripts, and update the line highlighted below with the values shown:

```
# Running on Linux.
IS_64BIT_JRE=`$JAVA_HOME/bin/java -version 2>&1 | grep "64-Bit"`
if [ "$IS_64BIT_JRE" = "" ]; then
ARCSIGHT_JVM_OPTIONS="-Xms128m -Xmx1024m"
export ARCSIGHT_JVM_OPTIONS
else
ARCSIGHT_JVM_OPTIONS="-Xms1024m -Xmx8192m" <======
export ARCSIGHT_JVM_OPTIONS
fi
;;
```

7. To ensure that MySQL shuts down gracefully in , edit the mysql_ctl file in /opt/arcsight/logger/current/arcsight/service and change this line:

```
STOPCMD="kill -9"
```

to this:

```
STOPCMD="kill "
```

Include the space after kill.

8. Increase the maximum capacity for session lists. Run the following command in the /opt/arcsight/logger/current/arcsight/bin directory:

```
./mysql -u <username> -p<password>
```

<username> and <password> are the database user name and password, as set when you configured the database, typically by using the First Boot Wizard.

Per MySQL conventions, omit the space between -p and the password, as shown in the following example:

```
./mysql -u arcsight -parcsight
```

In the resulting MySQL prompt, enter the following MySQL instructions:

```
use <ESM database name>;
update arc_session_list set in_memory_capacity=5000000 where resource_based_type=56;
commit;
quit;
```

Note that `in_memory_capacity` is set to 5,000,000.

9. Restart the ESM Manager for the new settings to take effect, by running the following command in the /sbin directory:

```
/sbin/service arcsight_services start manager
```

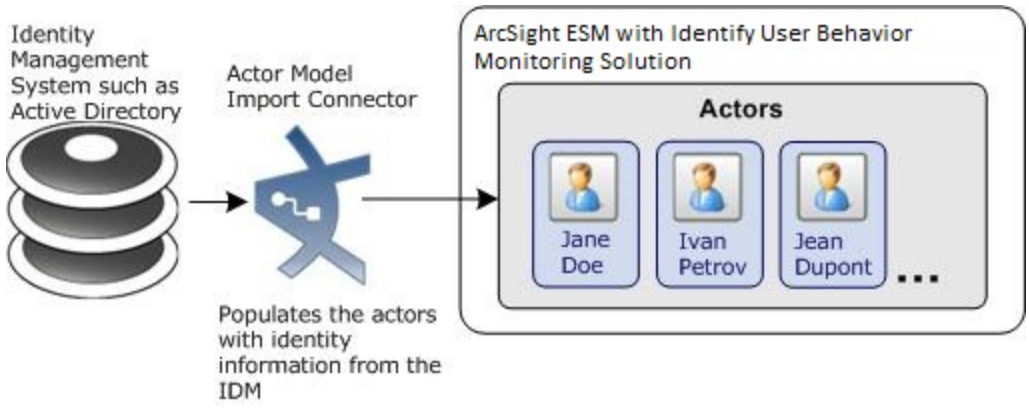
Install and Configure the Actor Model Import Connectors

Install and configure a supported version of the Active Directory Actor Model Import Connector, as described below.

1. Locate the installation file(s) for the Actor Model Import connector and the Actor Model Import Connector Configuration Guide downloaded from the support site.
2. Follow the instructions in the Configuration Guide to install and configure Actor Model Import connector. Note that there are configuration steps prior to connector installation as well as after connector installation.

ArcSight recommends that the clocks of the following systems are synchronized to an NTP source:
-System that hosts the Actor Model Import connector
-System that hosts the ESM Manager
-System that hosts the Domain Controller
If you are unable to synchronize using an NTP source, make sure the system time of the machine hosting theESM Manager is ahead of the system time for the machine hosting the Actor Model Import connector.

3. Follow the instructions in the Configuration Guide to populate the actors in ESM from the Identity Management System.



4. You can verify that the actors were imported into ESM Manager:

- From the ESM Console, go to the Navigator panel and go to Actors.
- Verify that actors are listed in the /Actors/Shared/All Actors group.

Configure Event Connectors to Return Uppercase User Names

Configure all the event (device) connectors that supply UBM-relevant events to return the user names in uppercase. When the Actor Model Import connector(s) populate the user names in actors, it converts all the account user names to uppercase. In order for the account user names in the events to match the account user names stored in the actors, you must configure the connector to return the user name in uppercase.

To configure an event connector to supply user names in uppercase:

1. In the Navigator panel, go to **Connectors**.
2. Right-click a Connector and select **Configure**.
3. In the Inspect/Edit panel, select the **Default** tab.
4. In the Processing panel for the Uppercase User Names field, select the **Enabled (orig to ID)** option.
5. Repeat this procedure for all event connectors.

Install the UBM Solution

Follow the procedure below to install the UBM solution.

Important: You cannot upgrade IdentityView to UBM 2.8. You must back up and uninstall the package. Then delete the package from the resource list. See Back Up and Uninstall for more details.

To install the UBM Solution package:

1. Download the following package to the machine where you plan to run the ArcSight Console:

ArcSight-SolutionPackage-UBM.<nnnn>.0.arb

Where <nnnn> is the four character build number specified in the ArcSight User Behavior Monitoring 24.3 Release Notes.

If you use Internet Explorer to download the ARB file, it might convert the ARB file to a ZIP file. If this occurs, rename the ZIP file back to an ARB file before importing.

2. Log into the ESM Console with an account that has administrative privileges.
3. Click the **Packages** tab in the Navigator panel.

4. Click Import ( ).
5. In the Open dialog, browse and select the package file and select **Open**.

The progress of the import of the package is displayed in the Progress tab of the Importing Packages dialog.

When the import is complete, the Results tab of the Importing Packages dialog is displayed as well as the Packages for Installation dialog.

6. Leave the UBM 24.3 checkbox selected.
7. In the Packages for Installation dialog, click Next.

The progress of the install is displayed in the Progress tab of the Installing Packages dialog. When the install is complete, the Results tab of the Installing Packages dialog displays the Summary Report.

8. In the Installing Packages dialog, click **OK**.
9. In the Importing Packages dialog, click OK.
10. To verify that the installation was successful and the content is accessible in the Navigator panel, expand the ArcSight Solutions/UBM package resource.
11. Optional—After you import actors with the Active Directory Actor Model Import SmartConnector, verify that the actors are populated by viewing the actors in the Actor Changes dashboard:
    a. In the Navigator panel Resources tab, select **Dashboards** from the drop-down menu.
    b. Navigate to ArcSight Solutions/UBM/Actor Management/.
    c. Right-click Actor Changes and select **Show Dashboard**.

Installation Troubleshooting

If the installation was not successful, contact ArcSight technical support for assistance.

Upgrade the UBM Package from UBM 2.7 to 2.8

Important: You cannot upgrade IdentityView to UBM 2.8. You must back up and uninstall the package. Then delete the package from the resource list. See Back Up and Uninstall for more details.

1. Once you have downloaded the new .zip file from OpenText Downloads, complete the following steps.
2. Extract the zipped files.
3. Go to the ArcSight Console.
4. Click Packages.
5. Click Import.

6. Select the .arb that matches the .arb from the unzipped file.
7. Follow the prompts to install the new package.

Assign User Permissions

By default, users in the Default user group can view UBM content, and users in the ArcSight Administrators and Analyzer Administrators user groups have read and write access to the UBM solution content. Depending on how you have set up user access controls within your organization, you might need to adjust those controls to make sure the new content is accessible to the right users in your organization.

The following process assumes that you have user groups set up and users assigned to them.

In the following procedure, assign user permissions to all the following resource types:

- Active channels
- Active lists
- Cases
- Category Models
- Dashboards
- Data monitors
- Global variables
- Field Sets
- Filters
- Integration Commands
- Integration Configurations
- Integration Targets
- Patterns
- Profiles
- Queries
- Query Viewers
- Session Lists
- Snapshots
- Trends
- Reports
- Rules

- Session Lists
- Use Cases

To assign user permissions:

1. Log into the ESM Console with an account that has administrative privileges.
2. For all the resource types listed above, change the user permissions:
   a. In the Navigator panel, go to the resource type and navigate to ArcSight Solutions/UBM.
   b. Right-click the **UBM** group and select **Edit Access Control** to open the ACL editor in the Inspect/Edit panel.
   c. In the ACL editor in the Inspect/Edit panel, select which user groups you want to have which permissions to the UBM active channels and click **OK**.

Configure UBM Solution

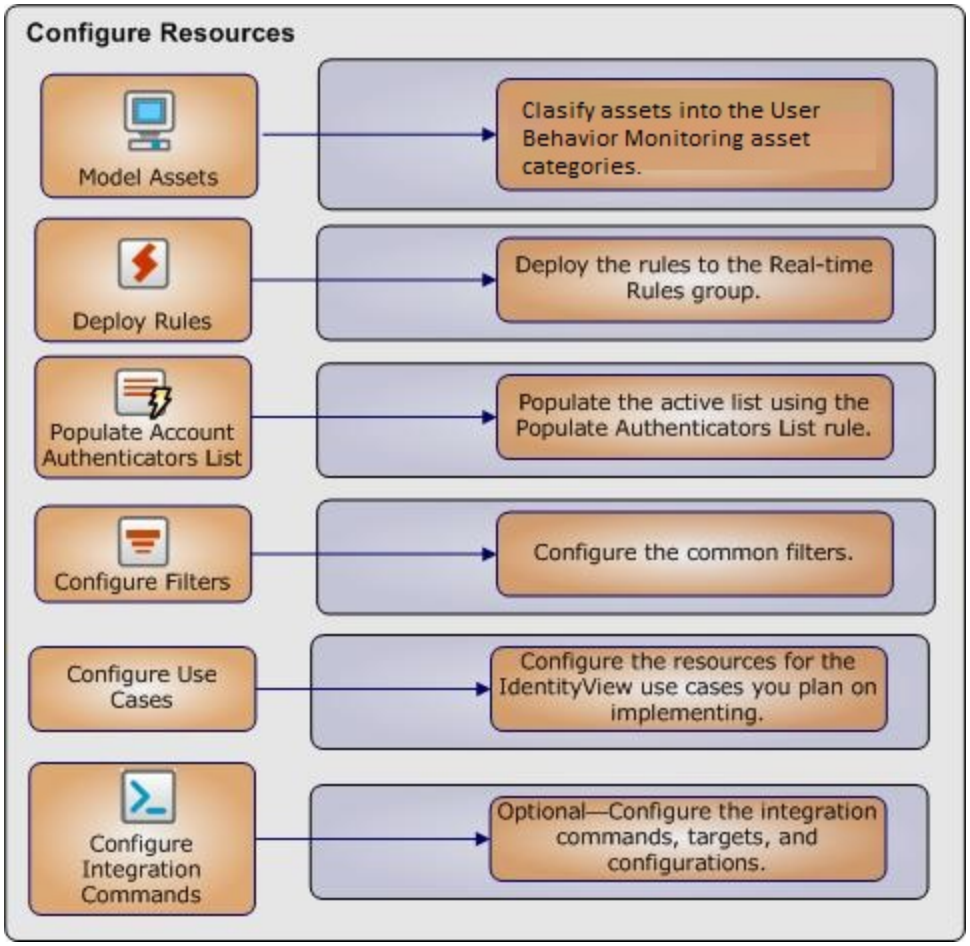
Several of the UBM solution resources should be configured with values specific to your organization. This section describes these configuration processes.

Depending on the features you want to implement and how your network is set up, some configuration is required and some are optional. The list below shows all the configuration tasks involved with the UBM solution and where to find instructions for performing the configuration.

This section contains the instructions required to enable content for the UBM solution and contains the following topics:

The configuration processes outlined in this section (shown in the figure below) apply to resources that feed multiple UBM use cases.

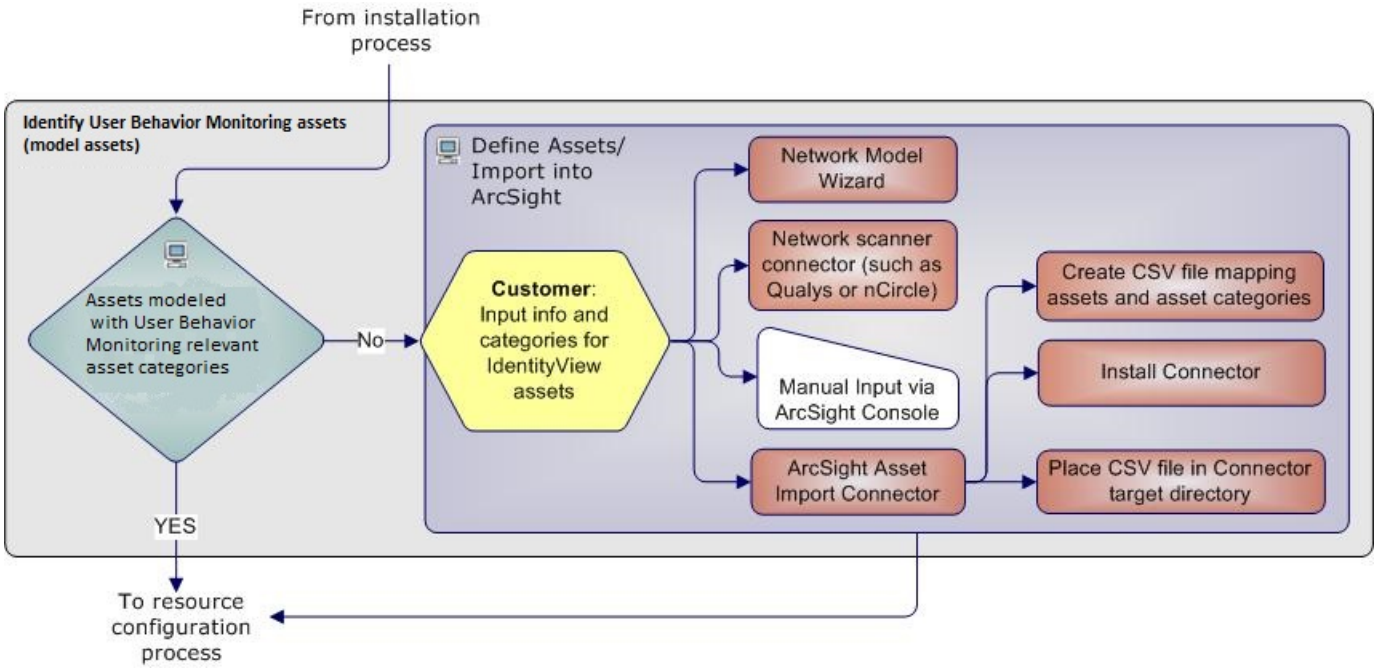
Configure Resources



Model Assets (Assign Asset Categories)

Asset modeling is essential to activate UBM solution content. Classifying assets in one or more of the UBM asset categories adds valuable business context to the events evaluated by the UBM solution.

Model Assets



The most important systems in the network should be classified with the Network Domain asset categories.

This taxonomy is extensible, so you can add your own asset categories within these UBM groups. If you create your own groups, or modify the name of an existing group, you might have to modify some UBM content to make use of them.

How to Assign Asset Categories

The UBM asset categories can be assigned using one the methods described here:

One by One Using the Console UI

Use this method if you have only a few assets to categorize. One asset can be categorized in more than one UBM asset category.

To categorize your assets one-by-one:

1. In the Navigator panel, go to Assets, select the Assets tab.
2. Expand the groups listed in the Asset tab.
3. For each asset you wish to classify with a UBM asset category, repeat the following steps:
   a. Right-click the asset you wish to categorize and select **Edit Asset**.
   b. In the Inspect/Edit panel, click the **Categories** tab. Click the add icon ( ) at the top of the screen to select new resources.

c. In the Asset Categories Selector pop-up window, navigate to the appropriate network domain category and click **OK**.

Once you have assigned your assets to the UBM asset categories, you can also assign them to other asset categories, either within the solution package or the general ArcSight categories, or those you have created yourself.

ArcSight Asset Import Connector

If you have many assets that you want to track, you can configure them in a batch using the ArcSight Asset Import Connector. This connector can also create new assets as part of the batch function.

The ArcSight Asset Import Connector is available as part of the SmartConnector download. For instructions about how to use this connector to configure your assets for UBM solution, see the ArcSight Asset Import Connector.

Network Model Wizard

The Network Model Wizard is provided on the ESM Console (menu option Tools | Network Model). The Network Model Wizard provides the ability to quickly populate the ESM network model by batch loading asset and zone information from Comma Separated Files (CSV) files. For more information, see the ArcSight Console User's Guide.

Deploy the UBM Rules

In order for the UBM solution to process UBM events, the UBM rules must be deployed to the Real-time Rules group.

To deploy the UBM rules:

1. From the Resources tab in the Navigator panel, go to Rules and navigate to the ArcSight Solutions/UBM group.
2. Right-click the UBM group and select Deploy Real-time Rule(s).

A new Real-time Rules/ArcSight Solutions/UBMgroup is created that is a link to the original ArcSight Solutions/UBM group.

For more information, see the ArcSight Console User's Guide.

3. As part of the use case configuration, enable only the rules for the use cases you want to implement. By default, the UBM solution rules are disabled. The UBM solution rules do not trigger until they are deployed and enabled. For detailed instructions on enabling and configuring the use case rules, see the Configure Resources section of each use case in "ArcSight User Behavior Monitoring Use Cases" on page 40.

Populate Account Authenticators List

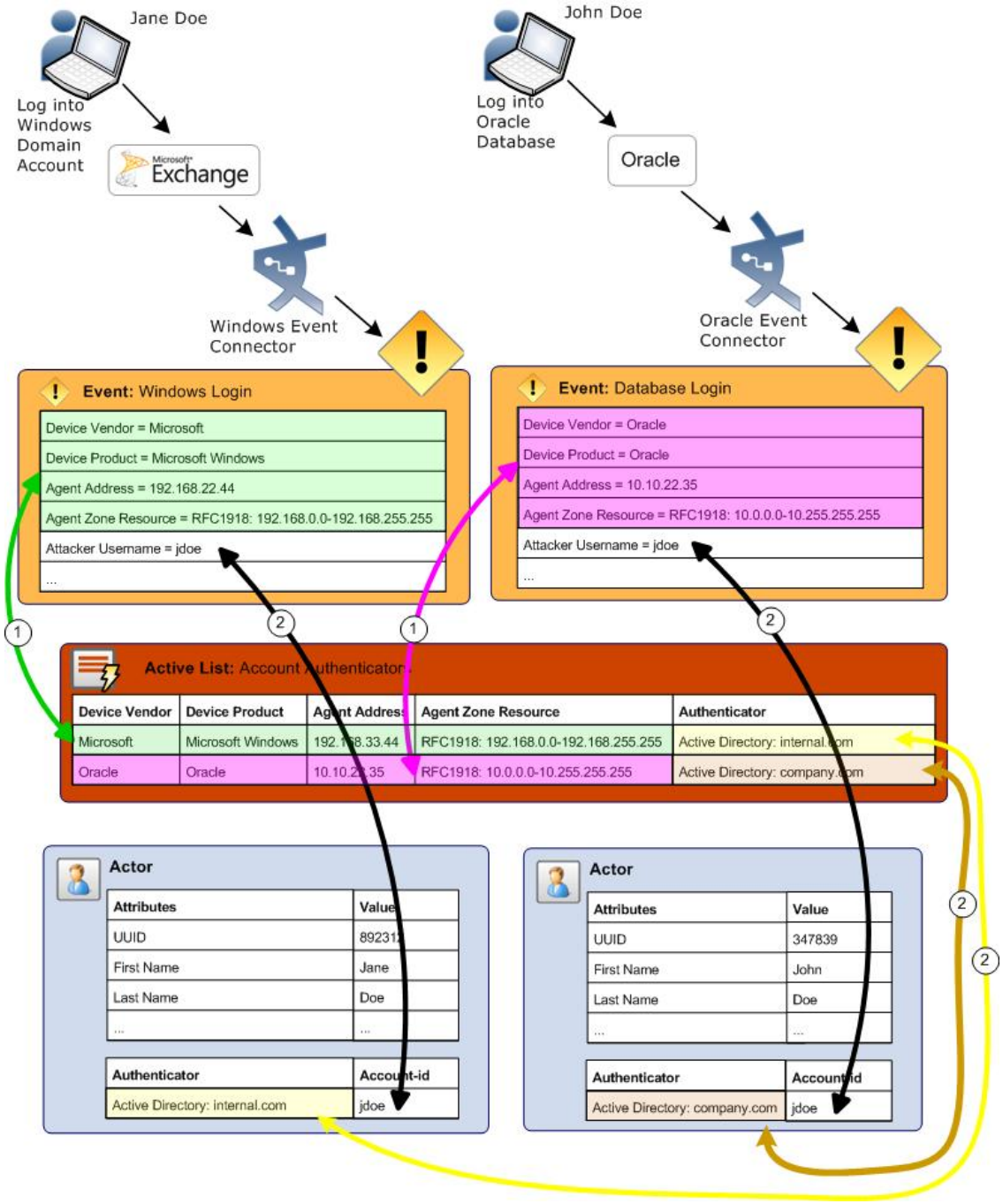
Populate the Account Authenticators List active list in ESM with the list of account authenticators used in your organization. The Account Authenticators List active list is used to uniquely qualify account IDs imported from

multiple authentication systems and seen in events. This list provides a way to correlate an account ID to the correct actor as shown the figure below. For example, the Windows connector collects events from an application that uses the Authenticator called Active Directory: internal.com, while the Oracle connector collects events from an application that uses the Authenticator called Active Directory: company.com. The active list tells the UBM solution which authenticator to use to look up an actor based on which event connector is reporting the event.

The following steps show how an event generated from activity from a jdoe account is correlated to the correct actor even though two jdoe accounts generate events in the environment. As shown in , Jane Doe logs into a Window Domain using the account jdoe and John Doe logs into an Oracle database using the account jdoe. (The steps listed below correspond to numbered circles in the diagram.)

1. The Windows Login event is correlated to the appropriate authenticator by matching the attributes of the event (shown highlighted in green) to the appropriate entry in the Account Authenticator List active list. In addition, the Database Login event is correlated to the appropriate authenticator by matching the attributes of the event (shown highlighted in pink) to the appropriate entry in the Account Authenticator List active list.
2. Using the user name specified in the event and the appropriate authenticator identified by matching attributes, the UBM solution determines the correct actor associated with each event.

Correlating Account IDs to Actors



Detailed instructions for populating this list manually are provided in the ArcSight Console User's Guide. The UBM solution also provides the rule to help you populate the ArcSight System/Actor Data Support/Account Authenticators active list with the account authenticators for each device as described in the following procedure.

To use the Populate Authenticators rule to populate the Account Authenticators active list:

1. Find the exact string that identifies the authenticator used by the most connectors in your organization:
   a. In the Navigator panel, go to Dashboards.
   b. Navigate to ArcSight Solutions/UBM/Actor Management/Actor Overview.
   c. Right-click the Actor Overview dashboard and select the Show Dashboard option. Make a note of the exact value of the Authenticator string including any punctuation, spaces, and capitalization, for example: Active Directory: <domain>.com.
2. In the Navigator panel, go to **Rules**.
3. Navigate to ArcSight Solutions/UBM/BookKeeping.
4. Right-click the Populate Authenticators List rule and select the **Edit Rule** option.
5. Select the **Local Variables** tab.
6. Double click the Expression field of the setDefaultAuthenticator row.
7. In the String field of the Arguments sub-panel, replace set-actor-authenticator-here string with the authenticator string you noted in and click **OK**.
8. Click OK.
9. In the Navigator panel, right-click the rule and select the Enable Rule option.

The rule looks for events generated from all devices for the specified authenticator and adds entries into the Account Authenticators active list for each device generating events. Each entry created specifies the default authenticator you specified in Step 7.

10. Wait until the ESM Manager receives events from every device for the specified authenticator in your environment.

If receiving events from every device in your environment takes more than one day, you can add the remaining entries manually and disable the rule. The rule is resource intensive because it compares every event to entries in an active list.

11. If your organization has more than one authenticator, edit the ArcSight System/Actor Data Support/Account Authenticators active list and for each of the devices that use a different authenticator, edit each entry and change the value of the Authenticator field to the correct value.
12. After populating the Account Authenticator List active list, disable the rule. The rule is resource intensive because it compares every event to entries in an active list.

Configure Common Filters

Configure the following common filters stored in the My Filters group to reflect your organization.

After Hours Filter

Defines the time period which is considered to be after business hours. The default after hours time period is set to 8:00 p.m. to 6:00 a.m. on weekdays, and all day Saturday and Sunday.

The filter uses two local variables:

- DayOfWeek
- HourOfDay

You can change this filter to match what is considered to be after-hours for your organization.

The DayOfWeek variable returns an integer value that is displayed on the ESM Console as a string value of the current day: Saturday, Sunday, Monday, Tuesday, Wednesday, Thursday, or Friday.
The HourOfDay variable returns a numerical value for the current hour in 24-hour format ranging from 12 AM = 0 to 11 PM = 23.

Attacker/Target Username is a System Account Filters

Selects events in which the attacker or target username are system accounts. These filters are designed to return events which can only be attributed to system or default accounts such as SYSTEM, ANONYMOUSLOGON, NETWORK SERVICE, NT AUTHORITY, -, or containing the character:$. Configure this filter with additional system accounts for your organization, by adding additional conditions.

Confidential Documents Filter

Defines the names of confidential documents. Edit the filter and add the file names of confidential documents.

Suspicious Documents Filter

Ddefines the names of suspicious documents. Edit the filter and add the file names of suspicious documents.

Actor Attribute Filters

Customize the following filters to reflect the values used in your organization.

Employee Type - Contractor Filter

Selects events that are attributable to contract employees. Edit the filter and specify the value(s) used to denote contractors in your organization.

Employee Type - Full Time Filter

Selects events that are attributable to full time employees. Edit the filter and specify the value(s) used to denote full time employees in your organization.

Employee Type - Part Time Filter

Selects events that are attributable to part time employees. Edit the filter and specify the value(s) used to denote part time employees in your organization.

Role - DBA Filter

Selects events attributable to actors having an administrative role such as administrator or dba. Configure this filter with any additional administrator roles used in your organization.

Status - Deleted Filter

Selects events in which the actor associated with the attacker or target user name has been deleted. Edit the filter and specify the value used to denote deleted identities in your organization.

If the Actor Model Import Connector detects that a user was deleted in the Identity Management System, the corresponding actor is not be deleted on the ESM Manager. Instead, the status attribute of the actor is set to Deleted in IDM.

Status - Disabled Filter

Selects events in which the actor associated with the attacker or target user name has been disabled. Edit the filter and specify the value used to denote disabled identities in your organization.

Run Integration Commands

The UBM solution provides integration commands that are invoked from the ESM Console and run on external web applications and ArcSight Logger appliances.

When a UBM solution integration command is run against an event, it derives identity data from the event, processes that data with a global variable, and passes the result into an external web application and Logger appliance.

Note:
The following behavior regarding events cannot be attributed to an actor: when a UBM Logger integration command is run against an event and the event cannot be attributed to an actor, the search criteria is empty and Logger returns all events.

The integration commands provided with the UBM solution only support investigating events listed in an active channel.

To run a UBM solution integration command:

1. In the Navigator panel, go to **Lists** and browse for an active channel that is receiving events.
2. Right-click an event in the active channel and select the Integration Commands | UBM <Type> where <Type> equals User Lookup, or Logger.

3. In the dialog, select the appropriate command, the target, and click OK. If values are not specified for all the parameter, the Parameters dialog displays.
   a. Enter values for the input parameters.

> **Note:** If you see a parameter name with underscores and a number such as AttributableActor____9, this is expected. The underscores and number specify an attribute. For example, the string AttributableActor____9 specifies the AttributableActor.Full Name attribute.

The following table provides parameter information for some integration commands.

Integration Commands	Parameter Information
• User Lookup by Actor Full Name • User Lookup by Event Full Name	For these commands, the following parameters specify the URL to the web application: AppHost, AppPath and AppParam. For example to search Bing website for the Full Name of the actor associated with the event, specify the following values for the command: • Set AppHost equal to www.bing.com • Set AppPath equal to search • Set AppParam equal to q If the value of Jane Doe is returned from the AttributableActor.Full Name attribute, the following URL is invoked when the integration command is run: http://www.bing.com/search?q=Jane Doe **NOTE**: If you cannot construct the appropriate URL for your web application using the supplied parameters listed above, edit the integration command and customize the URL.
• Search for Events Associated with Actor Near When the Event Occurred • Search for Events Associated with the Actor over the Past Day	For these commands, there are two types of authentication methods for logging into an ArcSight Logger: Original Logger Authentication Method—This method is supported for all current and future releases of ArcSight Logger and uses the following set of authentication parameters: LoggerHost LoggerUser LoggerPassword One Time Password (OTP) Authentication Method—This method will be supported in a future release of Logger and uses the following set of authentication parameters: LoggerHost OTPUser OTPPassword LoggerPort For more information, see the ESM and Logger documentation. If available, the One Time Password (OTP) Authentication Method is the preferred authentication method.

4. You can optionally choose to save the parameter values at either the target level or user level:

- **Save To Target**—Parameter values are saved in the associated target and all the users on the ESM Manager can access the values stored in the target.
- **Save To User**—Parameter values are saved associated with the current ESM user and only the current user can access the saved values.

Click OK. The integration command is invoked.

For more information, see the ArcSight Console User's Guide.

Customize the Value Type Passed into the Command

For some integration commands, you might want to customize the value type that is passed to the web application or appliance. For example, when you run the integration command, the integration command invokes the global variable and specifies that the full name associated with that actor should be returned. The full name is then passed to the google search web application. If you would rather search for the email address associated with the actor, you can change the type of value returned by the global variable and passed back to the integration command as described in the following procedure.

To customize the return value:

1. In the Navigator panel, go to Integration Commands.
2. Select the Commands tab.
3. Browse for a UBM solution integration command such as ArcSight Solutions/UBM/External/.
4. Right-click the integration command and select Edit Command.
5. Click the value in the URL field and click ... .
6. Delete all the text after the = character including the $ character.
7. Leave the cursor after the = character and type the $ character. A dialog appears to select appropriate field.
8. Select the appropriate value to be returned by the global variable. For example to change the value returned by the global variable, select Global Variables | AttributableActor.Email Address.

Configure UBM Use Cases

Additional configuration might be needed for the individual resources associated with a use case. For more information, see ArcSight User Behavior Monitoring Use Cases.

This section provides the general use case configuration information.

View Use Case Resources

The UBM solution resources are grouped together in the ESM Console using use case resources. A use case resource provides a way to group a set of resources that help address a specific security issue or business requirement.

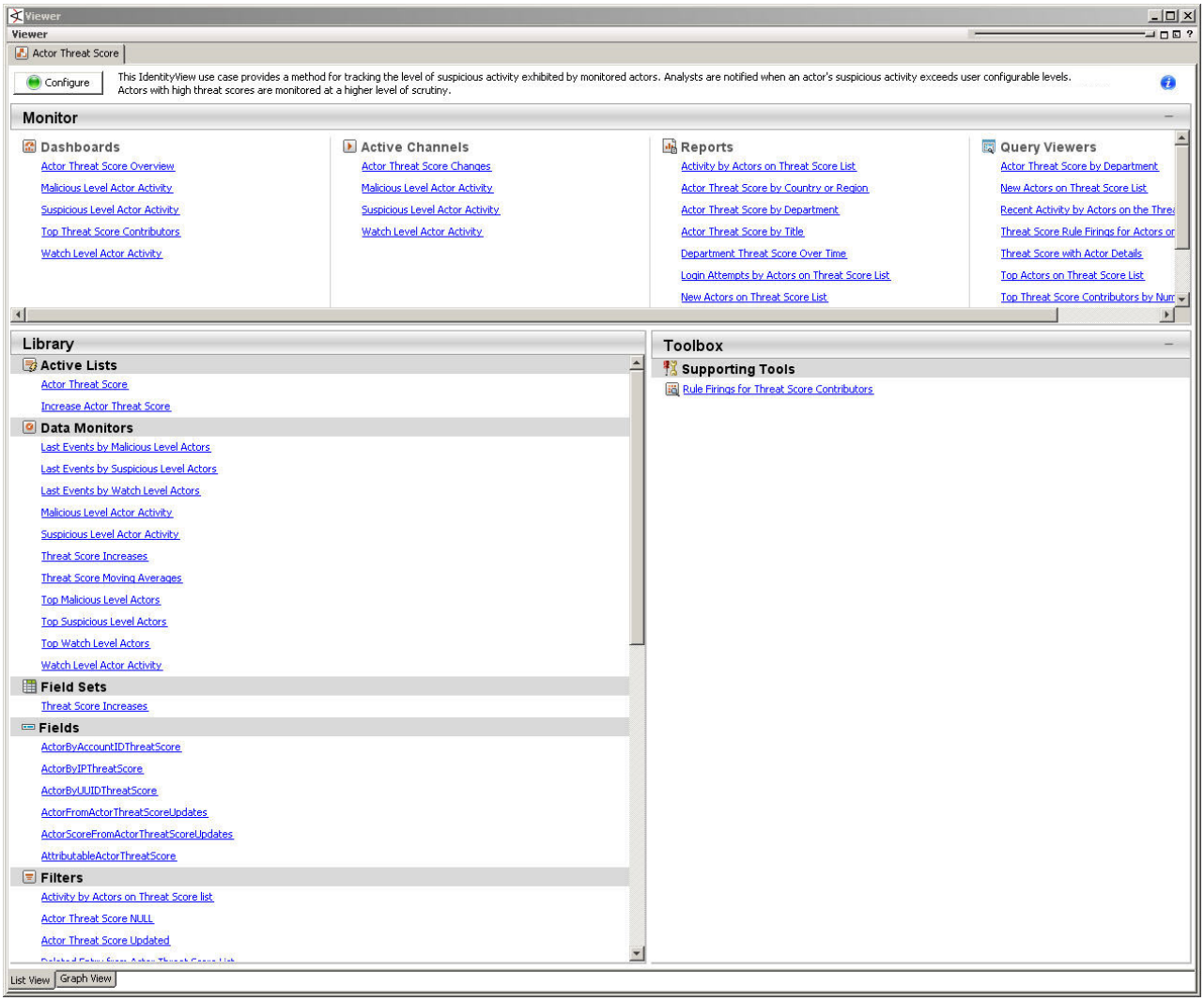
To view the resources associated with a use case resource:

1. In the Navigator panel select the **Use Cases** tab.
2. Browse for a UBM solution use case resource such as ArcSight Solutions/UBM/Actor Threat Score.
3. Right-click the use case resource and select the **Open Use Case** option.

The resources that make up a use case resource are displayed as shown in . The use case resource tables listed in ArcSight User Behavior Monitoring Use Cases. contain all the resources that have been explicitly assigned to the use case and any dependent resources used by the assigned resources.

The Configure Use Case option invokes a configuration wizard that is not currently supported for the UBM solution use cases.

Viewing the Resources Assigned to the Use Case



Configure Active Lists

You can populate UBM solution active lists manually using the following processes:

- Add entries to an active list, one-by-one, using the List Entry editor in the ESM Console.
- Add entries in batch to active list from a comma separated value (CSV) file.

Configure Lists Using Console Entry Editor

You can add entries to active lists, one-by-one, using the Entry editor of the ESM Console.

1. In the Navigator panel, go to Lists.
2. Select the Active Lists tab.
3. Navigate to ArcSight Solutions/UBM.
4. Right-click the list you wish to populate and select Show Entries. The list details are displayed in the Viewer panel.
5. For each entry you wish to add to the list, repeat the following steps:
   a. To add an entry to the list, click the Add icon in the list header.
   b. In the Entry editor of the Inspect/Edit panel, enter values for the required fields of the list and click Add.

Individual use cases might require additional active lists to be configured. For more information see the individual use case descriptions in ArcSight User Behavior Monitoring Use Cases.

Configure Active Lists by Importing a CSV File

Active lists can be populated in a single step, by importing entries from an existing CSV file. The number of columns in the active list must match the number of comma separated values in the CSV file. For example, if the active list has two columns of data, the imported CSV file must have two comma-separated fields.

1. In the Active Lists resource tree of the ESM Console, right-click an active list and choose Import CSV File. A file browser displays.
2. Browse to find the CSV file you want to import, select it, and click Open. The Import Preview dialog displays the data from the CSV file to be imported into the active list.
3. To add the entries from the selected file into the active list, in the Import Preview dialog, click OK. The new entries from the file are appended to the existing entries in the active list.
4. To verify that your entries were imported as expected, right-click the active list you just populated with the CSV file and select Show Entries.

This displays the newly-added data from the CSV file in the Viewer panel as active list details.

Individual use cases might require additional active lists to be configured. For more information, see ArcSight User Behavior Monitoring Use Cases.

By default, the active list displays 2000 entries at a time. To view entries outside the range shown, create an active list filter that specifies a different range (click Filter in the active list header).

Determine the UUID to Populate Active Lists

Some of the active lists require that you specify the Universally Unique Identifier (UUID) associated with an identity as specified by the Identity Management System. The UUID of identity is stored as an attribute in the actor and is used as the key to look up the other attributes of the identity. For example, the UUID of Jane Doe specified in the

active list, can be used by the UBM solution resources to look up the Employee Type attribute stored in the Jane Doe actor.

To get the UUID associated with an actor:

1. In the Navigator panel, go to **Actors**, and select the **Actors** tab.
2. Expand the groups listed in the **Actors** tab.
3. Right-click an actor and select **Edit Actor**. The UUID is displayed at the top of the Inspect/Edit panel in the Attributes tab.

Test Filters

Most of the content in the UBM solution relies on event categorization fields to identify events of interest. Although this method applies to most of the events and devices, for certain use cases, it is recommended that you test key filters to verify that they actually capture the required events. This section describes, generally, how to test filters. The following procedure should be performed only on a test (non-production) system.

To ensure that a filter captures the relevant events:

1. Generate or identify the required events and verify that they are being processed by ESM by viewing them in an active channel or query viewer.

To generate relevant events and send them to ESM, you can either:
1. Set up a connector to capture events from a target system and perform the actions that would generate the required events on that system. For example, to test the filter, set up a connector on a Microsoft Windows machine and login into the server.
or
2. Import into ESM an existing batch file that contains relevant events.
Alternatively, you can identify that these types of events have already been processed by ESM and ensure that the start and end time of the active channel or query viewer (as shown in) covers the event time of these events.

2. Navigate to the appropriate filter, right-click it, and then choose **Create Channel with Filter**. If you see the events of interest in the newly created channel, then you know that the filter is functioning properly.

If you do not see the events of interest:

- Verify that the configuration of the active channel is suitable for the events in question. For example, ensure that the event time is within the start and end time of the channel.
- Modify the filter's condition to capture the events of interest. After applying the change, repeat to verify that the modified filter captures the required events.

For a use case to process and display complete information, filters should capture similar events from different systems. For example, the filter should capture such events from both Microsoft and Unix systems.

Also, try to minimize false positives and negatives as much as possible. For example, the filter should capture a single event for every successful login attempt to a Unix machine, but not unsuccessful login events. To achieve this end, you might have to further fine tune the filter's condition.

Enable and Test Trends

By default, the UBM solution trends are not enabled. Many reports and query viewers require that trends be enabled to capture data shown in these monitoring resources. As part of the use case configuration, enable trends for the use cases you want to implement. Before enabling a trend, you should verify that trend captures data relevant for your environment as described in procedure below. In addtion before enabling a trend, you might want to also customize the following values:

- Schedule Range Start date in the Schedule tab of the Inspect/Edit panel—By default, the UBM trends collect data based on the installation time of the UBM 24.3 package on the ESM. Before enabling the trend ensure that the Start field of the trend on the Schedule tab reflects the date you want to start collecting events from.
- **Partition Retention Period (in days**) attribute— This attribute specifies the number of days to retain the partitions from this trend as active in the ArcSight database. You might want to increase Partition Retention Period (in days) attribute of the trend for your environment. This attribute is used in combination with the Partition Size. Note that reducing the partition retention period might case the use case not to function properly.

For more information about trends, see ArcSight Console User's Guide and the Trends sections in ArcSight User Behavior Monitoring Use Cases

To ensure that a trend captures the relevant events:

1. Generate or identify the required events and verify that they are being processed by ESM.

To generate relevant events and send them to ESM, you can either:
1. Set up a connector to capture events from a target system and perform the actions that would generate the required events on that system. For example, to test the filter, set up a connector on a Microsoft Windows machine and login into the server.
or
2. Import into ESM an existing batch file that contains relevant events.
Alternatively, you can identify that these types of events have already been processed by ESM and ensure that the start and end time of the active channel or query viewer (as shown in) covers the event time of these events.

2. Navigate to the appropriate trend, right-click it, and then choose Test. If you see the events of interest in the test panel, then you know that ESM is processing events that could be captured by the trend. The test panel

shows relevant events that could be captured by the trend in the last hour, up to 25 rows.

If you do not see the events of interest, you might want customize the queries invoked by the trend for your environment.

Configure Cases

Cases are ESM's trouble-ticket system that can be used as-is or in conjunction with a third-party trouble-ticket system. The UBM solution includes the ArcSight Solutions/UBM group, which holds the cases generated by UBM rules.

You can add more groups to the ArcSight Solutions/UBM group or your own group if you want to add more differentiations. If you do add more groups to the ArcSight Solutions/UBM group, modify the ESM Console rules that generate cases to use of your new case groups.

By default, some rules contain Add to Existing Case actions. These actions are triggered only if the action is enabled and the rule is both deployed and enabled.

If you want to generate cases for specific suspicious activities, you can edit rules that trigger on that specific behavior and add actions those rules to create cases. For example, if you want to create a case every time activity from rogue account occurs, edit the rule and add an action that creates a case.

Configure Notifications

You can add a rule action to UBM solution rules that send notifications when the rule is fired. In addition, you can create notification destinations that receive the notifications when the rules fire. For more information, including configuration information, see the ArcSight Console User's Guide. This configuration is optional. Additional information about configuring notifications for specific rules are described for individual use cases in this chapter.

Chapter 3: ArcSight User Behavior Monitoring Use Cases

The ArcSight User Behavior Monitoring (UBM) solution resources are organized in the ESM Console using use case resources. A use case provides a way to group and view a set of resources that help address a specific security issue or business requirement.

The UBM solution supports the use cases listed in the following table. Open Text recommends configuring the use cases in the order listed below to maximize the reporting information for the downstream use case. For example, configuring the Actor Attribution by IP Address Use Case before the Actor Threat Score Use Case means that the Actor Threat Score Use Case can attribute events to actors using IP addresses.

You can find more details about configuring each use case by clicking the use case's name in the table.

Use Case	Use Case Purpose
Actor Management Use Case	Contains resources designed to show analysts the status of actor resources in ESM. The number of actors, roles, and account IDs monitored can be identified with this use case. In addition, analysts can monitor changes to actor resources, and identify the use of rogue accounts that cannot be tied to any actor in ESM.
Actor Attribution by IP Address Use Case	Associates IP addresses to actors, and allows events from IP addresses to be attributed to the logged in actor, even if no username is present in the event.
Shared Accounts Use Case	Reports on the usage of accounts that might be in use by more than one individual. The use case can detect when anyone uses an existing known shared account, as well as detect the use of any account by more than one individual.
Actor Threat Score Use Case	Provides a method for tracking the level of suspicious activity exhibited by monitored users. Analysts are notified when an actor's suspicious activity exceeds configurable levels. Actors with high threat scores are monitored at a higher level of scrutiny.
Suspicious Activity Use Case	Contains resources that can be used to discover and analyze suspicious activity occurring on your network. When triggered, the suspicious activity rules can contribute to the resources of the Actor Threat Score Use Case.
User Activity Monitoring Use Case	Contains resources designed to enable analysts to monitor the activity of users on the network. Many resources break down activity by actors' employee type, department, or other attributes.
Privileged User Monitoring Use Case	Monitors the usage and authorization of privileged accounts.
Federations Services Use Case	Monitors Active Directory Federation Services (AD FS) activity for potential threats to your environment.

Actor Management Use Case

The Actor Management use case contains resources designed to show analysts the status of actor resources in ESM. The number of actors, roles, and account IDs monitored can be identified with this use case. In addition, analysts can monitor changes to actor resources, and identify the use of rogue accounts that cannot be tied to any actor in ESM.

The Actor Management use case monitors and reports on changes to actor information such as employee type, status, department, roles and account IDs. The Actor Model Import connector dynamically synchronizes information from an Identity Management System to the actors stored in ESM. By monitoring and reporting on the changes to actors, this use case effectively monitors changes to the Identity Management System.

If an account ID is not known by the Identity Management System and therefore not associated with any actors, the account ID is considered to be rogue. For example, if a database administrator creates an account in the database but does not register that account in the Identity Management System, the account ID is rogue. By comparing relevant actor information with events observed on the network, this use case can report when activity is observed from accounts which cannot be correlated to an identity—the activity of rogue accounts.

In addition, the resources provided in the Actor Management use case enable auditors, analysts, and managers to provide the following services:

- Monitor and report on role changes within the Identity Management System including when privileges are added or revoked from an actor
- Monitor and report on role groups including the actors that are assigned to a role
- Monitor and report the number of actors and roles and the breakdown of actors by organizational unit and department
- Generate authorization and role change reports per department for verification by responsible parties—to assist with role attestation
- Monitor and report when actors are added or deleted from the Identity Management System
- Monitor and report when actors are manually changed or deleted on ESM using the ESM Console
- Monitor and report the account IDs, applications and addresses associated with rogue accounts
- Monitor and report both the events that can and cannot be attributed to actors. For events that are attributed to actors, the method of attribution is reported: account ID or IP address.
- Detect patterns with actor attribute modifications, actor role deletions and additions

Configure Resources

Configure the following types of resources for this use case:

Rules

The following rules can be configured for this use case:

Enable the Actor Changes rule if you want to track the activity of rogue accounts—accounts IDs not attributable to any actors. (If enabled, this rule might trigger excessively if there are a lot of account IDs that are not in your actor model.)

If this rule is enabled and rogue account activity is detected, by default the rule invokes the following actions:

- **Add to Active List**—Adds the rogue account ID into the Actor Changes active list.**Set Event Field Actions**—Sets the agent severity to medium for the event generated by this rule and attempts to attribute the event to an actor by invoking the Actor Changes global variable.

By default, the other actions of the Actor Changes rule are disabled. You can optionally enable these actions:

- **Add to Existing Case**—Adds a case to the specified URI. For more information, see .
- **Send Notification**—If this action is enabled and the rule is triggered, the rule sends a notification to all users assigned to the CERT Team.

Enable the Actor Changes rule if you want to track when an actor resource is deleted using the ESM Console. Manually editing the information stored in actors should be avoided because typically this information is dynamically updated by Actor Model Import connector(s). If this rule is enabled and an actor resource has been deleted, by default the rule invokes the following actions:

- **Set Event Field Actions**—Sets the agent severity to high for the event generated by this rule.

By default, the other action of the Actor Changes rule is disabled. You can optionally enable this action:

- **Send Notification**—If this action is enabled and the rule is triggered, the rule sends a notification to all users assigned to the CERT Team. For more information, see .
- **Add to Existing Case**—Adds a case to the specified URI. For more information, see .

Enable the Actor Changes rule if you want to track when the identity information stored in actors has been manually changed using the ESM Console. Manually editing the information stored in actors should be avoided because typically this information is dynamically updated by Actor Model Import connector(s). This rule is provided to send a notification when someone edits actors manually. If this rule is enabled and ESM audit events indicating actor changes are detected, by default the rule invokes the following action:

- **Set Event Field Actions**—Sets the agent severity to low for the event generated by this rule.

By default, the following actions of the Actor Changes rule is disabled. You can optionally enable these actions:

Send Notification—If this action is enabled and the rule is triggered, the rule sends a notification to all users assigned to the CERT Team.

Add to Existing Case—Adds a case to the specified URI.

Devices

This use case depends on audit events generated by ESM when actor resources are modified. Any device can contribute to the Actor Changes rule. The Actor Changes rule is triggered by the account activity of rogue accounts from any device.

The Actor Changes and Actor Changes rules are triggered by audit events triggered by ESM.

All devices can supply events to this use case but the resources will only process events from devices, when the device generates events that can be attributed to specific actors.

Verify Configuration

After configuring this use case, verify that ESM is collecting events that indicate that actors are being populated by the Actor Model Import connector(s):

1. In the Navigator panel, go to **Dashboards**.
2. Navigate to ArcSight Solutions/UBM/Actor Management/.
3. Right-click Actor Changes and select **Show Dashboard**.

Resources

The following table lists all the resources explicitly assigned to this use case and any dependent resources. Each resource can be accessed from the Actor Management use case landing page: /All Use Cases/ArcSight Solutions/UBM/Actor Management, or their URI, for example: /All <Resource Type>/ArcSight Solutions/UBM/<Use Case>/<Resource Name>.

Resource	Description	Type
Monitor Resources		
Actor Changes	This active channel shows all actor audit events generated by ESM when an actor resource is updated.	Active Channel
Activity from Rogue Account IDs	This active channel shows correlation events that indicate the use of rogue account IDs.	Active Channel

Resource	Description	Type
Actor Role Changes	This active channel shows actor audit events indicating role changes have occurred.	Active Channel
Actor Roles Overview	This dashboard shows a summary of actor role data and can be used to investigate the current status of actor role assignments in the system.	Dashboard
Rogue Account IDs	This dashboard shows information associated with rogue accounts such as account IDs, applications, attacker addresses and target addresses.	Dashboard
Actor Role Changes	This dashboard displays several data monitors that can be used for monitoring changes to actors' role assignments.	Dashboard
Events with and without Actors	This dashboard shows a summary of how events over the last hour are being attributed to actors and includes information about those events that are not attributed to actors.	Dashboard
Actor Overview	This dashboard shows a summary of actor data and can be used to investigate the current status of actor resources in the system.	Dashboard
Actor Changes	This dashboard displays several data monitors that can be used for monitoring changes to actor resources that are imported by model import connectors, or via manual changes.	Dashboard
Role Names	This query viewer shows every role name and role type in the system, ordered by role name.	Query Viewer
Number of Role Assignments	This query viewer displays the total number of actor role assignments per authenticator in the system.	Query Viewer
Count of Roles by Type	This query viewer displays the number of roles of each type in the system.	Query Viewer
Leaf Node Organizational Units	This query viewer shows the leaf node organizational unit from actors' distinguished names, and the number of actors in that organizational unit.	Query Viewer
Number of Account IDs	This query viewer displays the number of unique account IDs per authenticator in the system.	Query Viewer
Top 20 Roles	This query viewer displays the top roles by count of the actors assigned to them.	Query Viewer
Roles by Actor	This actor query viewer shows every actor's full name and roles.	Query Viewer
Top Rogue Account IDs in Use	This query viewer shows the top rogue account IDs by count of the number of events. Each rogue account ID is a combination of the attacker and target user names.	Query Viewer
Department Overview	This query viewer displays the number of actors in each department.	Query Viewer
Top Attacker Addresses with Activity from Rogue Account IDs	This query viewer shows the top attacker addresses by count of the number of events that show activity attributable to rogue accounts IDs.	Query Viewer

Resource	Description	Type
Top Target Addresses with Activity from Rogue Account IDs	This query viewer shows the top target addresses by count of the number of events that show activity attributable to rogue accounts IDs.	Query Viewer
Actor Status Overview	This query viewer displays each unique actor status value and the number of actors having that status.	Query Viewer
Top Applications with Activity from Rogue Account IDs	This query viewer shows the top applications by count of the number of events that show activity attributable to rogue accounts IDs.	Query Viewer
Top 20 Actors with Roles	This query viewer displays the top actors by count of their role assignments.	Query Viewer
Actor Base Attributes	This query viewer displays all single-value attributes (base attributes) for each actor in the system.	Query Viewer
Total Number of Actors	This query viewer displays the number of unique actor resources in the system.	Query Viewer
Count of Roles by Memberships	This query viewer gives the number of actors that are assigned to each role.	Query Viewer
Actors	Offers comprehensive insights into actors registered on ESM. It includes: • A detailed listing of actors categorized by their identity management identifiers. • A speedometer chart illustrating the current availability status of actors within ESM. • A bar chart showcasing the distribution of actors across different identity management identifiers.	Report
Detailed Activity for Account ID	This report shows all activity that can be attributed to a single account id.	Report
Actors with Specified Role	This report shows all role assignments for actors having the role specified when running the report. The report lists each actor having the specified role, and all of the other roles assigned to each actor.	Report
Rogue Account IDs - Activity	This report shows a summary of all events attributable to rogue accounts and can be used to identify the use of rogue accounts on specific systems.	Report
Role Attestation for Department	This report shows all roles for actors in the specified department.	Report
Top Rogue Account IDs in Use	This report shows the top rogue account IDs by count of the number of events. Each rogue account ID is a combination of the attacker and target user names.	Report
Actor Role Changes	This report shows a summary of actor role changes, included role added and role deleted events.	Report
Roles by Number of Assignees	This report shows each role, role type, and the number of actors assigned to that role.	Report
Role Attestation for All Actors	This report shows all roles for all actors in the system that have a status of Active.	Report

Resource	Description	Type
Rogue Account IDs - List	This report shows a list of the rogue account IDs included on the Rogue Account IDs active list.	Report
Role Attestation for Actors with Specified Role	This report shows all role assignments for actors having the role specified when running the report. The report lists each actor having the specified role, and all of the other roles assigned to each actor.	Report
Actors Status Disabled	This report shows information from actor audit events indicating an actor's status was set to disabled.	Report
Actor Information Detail	This report shows a detail of the attributes for all actors in the system.	Report
Actors Added	This report shows information from actor audit events indicating an actor resource was added to the system.	Report
Library - Correlation Resources		
Activity from Rogue Account ID	This rule triggers on events attributable to rogue account IDs, and adds the account IDs to the Rogue Account IDs active list.	Rule
Actor Updated by Interactive Session	This rule triggers on actor audit events generated by ESM when an actor resource is updated by an interactive session, such as an admin user session. Its purpose is to notify when manual changes are made to actor resources.	Rule
Actor Deleted by Interactive Session	This rule triggers on actor audit events generated by ESM when an actor resource is deleted by an interactive session. Its purpose is to notify when manual deletions of actor resources occur.	Rule
Library Resources		
My DNS Domains	This active list defines the DNS domain names which are owned by the organization.	Active List
Rogue Account IDs	This active list contains relevant information from events that involve the use of a rogue account id.	Active List
Account Authenticators	This active list is used by the actor global variables to determine what the Identity Management authenticator is, base on the event, so that an actor can be determined from event information.	Active List
Known Shared Accounts	This active list maintains a list of known shared accounts per application. Note that all account IDs must be in uppercase and the Application field must be the same as what appears in the Device Product event field.	Active List
Top 20 Departments	Displays the number of actors in each department.	Data Monitor
Top 20 Locations	Displays the number of actors in each location	Data Monitor
Actor Audit Events - Top Actions	This data monitor calculates the most frequent actions being taken on actor resources.	Data Monitor

Resource	Description	Type
Actor Role Deletions - Last N	This data monitor maintains a list of the last n actor role deletions.	Data Monitor
Actor Audit Events - Top Actors	This data monitor calculates the most frequent actor resources being updated.	Data Monitor
Actor Role Additions - Last N	This data monitor maintains a list of the last n actor role additions.	Data Monitor
Actor Attribute Updates	This data monitor maintains a list of the last n actor attribute change events.	Data Monitor
Actor Role Additions - Top Value Counts	This data monitor calculates the most frequent role assignments added to actor resources.	Data Monitor
Actor Audit Events - Interactive Session	This data monitor shows pertinent fields from actor audit events caused by an interactive session, such as admin user.	Data Monitor
Events without Actors - Top 10 Usernames (Last Hour)	This data monitor shows the top 10 user names across events that cannot be attributed to an actor in the last hour.	Data Monitor
Actor Account ID Additions	This data monitor maintains a list of the last n actor account ID additions.	Data Monitor
Events with and without Actors in the Last Hour	This data monitor shows a moving average of how many events can and cannot be attributed to an actor.	Data Monitor
Actor Role Deletions - Top Value Counts	This data monitor calculates the most frequent role assignments deleted from actor resources.	Data Monitor
Actor Account ID Deletions	This data monitor maintains a list of the last n actor account ID deletions.	Data Monitor
Events with no Actor Breakdown by Authenticator (Last Hour)	This data monitor shows a moving average of how many events cannot be attributed to an actor by authenticator. In case an authenticator cannot be derived from an event, the device vendor, product, agent address and agent zone event fields are displayed.	Data Monitor
Events with Actors Breakdown - Last Hour	This data monitor shows a breakdown of how actors are being mapped to events either by account (event user name) or by the originating IP address.	Data Monitor
solnConcatAttackerTargetUser	This variable concatenates the attacker user name, a | character and the target user name. It can be used as a single field to showcase various user name combinations in events.	Global Variable
ARST_IDV_ DeletedAccountResource	This global variable returns the deleted account ID resource from actor audit events.	Global Variable
ActorByAccountID	This global variable maps the account information in an event with an actor. The account information consists of the device vendor and product, and information derived from the attacker or target user name, with preference to the target user name.	Global Variable
ActorFromIPMap	This global variable returns an actor's UUID, full name, username used, and login type if the actor is associated with a source IP address.	Global Variable

Resource	Description	Type
ARST_IDV_ActionFromAuditEvt	This global variable returns the action type from actor audit events.	Global Variable
ARST_IDV_DeletedResource	This global variable returns the deleted role resource from actor audit events.	Global Variable
ARST_IDV_AddedAccountID	This global variable returns the added account ID from actor audit events.	Global Variable
AttributableActor	This global variable returns all the information for an actor, where the event to actor attribution is done using either attacker or target user name fields, or the source IP address. Note: To turn lookups based on the source IP address, in the Parameters tab, do not use the actorByAccountOrSourceIP local variable to lookup the actor, use the UUID field of the ActorByAccountID global variable instead.	Global Variable
ActorByIP	This global variable returns all the information for an actor, where the event to actor attribution is done using the source IP address.	Global Variable
ARST_IDV_ AddedAccountResource	This global variable returns the added account ID resource from actor audit events.	Global Variable
Top Level OUs	This global variable returns the top level OU from an actor's distinguished name.	Global Variable
ActorByAttackerUserName	This variable maps the account information in an event with an actor. The account information consists of the device vendor, device product, connector address, connector zone, and information derived from the attacker user name.	Global Variable
solnPatternDiscoveryConst	This variable returns a constant string that can be used in Pattern Discovery profiles when it is not required to specify either a Source or a Target event field.	Global Variable
ARST_IDV_DeletedAccountID	This global variable returns the deleted account ID from actor audit events.	Global Variable
ActorByTargetUserName	This variable maps the account information in an event with an actor. The account information consists of the device vendor, device product, connector address, connector zone, and information derived from the target user name.	Global Variable
ARST_IDV_DeletedRole	This global variable returns the deleted role from actor audit events.	Global Variable
solnGetAuthenticator	This global variable extracts the authenticator from the event by looking up the Account Authenticators list using event fields.	Global Variable
solnGetUsername	This global variable returns user name in an event from target user name or attacker user name, with preference to the target user name.	Global Variable
ARST_IDV_ActorFromAuditEvt	This global variable returns the modified Actor from actor audit events.	Global Variable

Resource	Description	Type
ARST_IDV_AddedRole	This global variable returns the added role from actor audit events.	Global Variable
ARST_IDV_AddedRoleType	This global variable returns the added role type from actor audit events.	Global Variable
ARST_IDV_AddedResource	This global variable returns the added role resource from actor audit events.	Global Variable
ARST_IDV_ActorsManager	This global variable retrieves an actor's manager actor, by using the Manager DN field of the subordinate actor resource.	Global Variable
ARST_IDV_ UpdatedAttributeValue	This global variable returns the updated attribute new value from actor audit events.	Global Variable
ARST_IDV_ UpdatedAttributeName	This global variable returns the updated attribute name from actor audit events.	Global Variable
ARST_IDV_DeletedRoleType	This global variable returns the deleted role type from actor audit events.	Global Variable
Activity from Rogue Account IDs	This field set selects pertinent fields from events attributable to rogue account IDs.	Field Set
Actor Role Additions	This field set contains fields of interest for monitoring additions to Actors assigned roles.	Field Set
Actor Audit Events	This field set contains fields of interest for monitoring changes to Actor resources.	Field Set
Actor Role Deletions	This field set contains fields of interest for monitoring deletions from Actors assigned roles.	Field Set
ActorByTargetUserName is NULL	This filter selects events which cannot be attributed to an actor based on the target user name field.	Filter
Target Username is a System Account	This filter selects events in which the target user name is a system account.	Filter
ActorByAttackerUserName is NULL	This filter selects events which cannot be attributed to an actor based on the attacker user name field.	Filter
All Failed Logins	This filter selects all events indicating that a user failed authentication.	Filter
Target User Name is Rogue Account ID	This filter selects events that the target user name is unknown and cannot be associated to actors or other predefined accounts.	Filter
ActorByIP is NULL	This filter selects events where an actor cannot be attributed to an event based on the event source IP address.	Filter
Attacker User Name is a System Account	This filter selects events in which the attacker user name is a system account.	Filter
ASM Events	This filter selects internal monitoring events involving data monitor resources.	Filter

Resource	Description	Type
Actor Audit Events by Interactive Session	This filter selects actor audit events generated by ESM when an actor resource is updated by an interactive session, such as admin user. Its purpose is to find manual changes made to actor resources.	Filter
Actor Audit Events - Account Identifier Deleted	This filter selects actor audit events generated by ESM when an actor's account ID is deleted.	Filter
Outbound Email	This filter selects events indicating email traffic from internal domains to external domains.	Filter
ArcSight Events	This filter selects events in which the Device Vendor and Device Product is ArcSight.	Filter
Attacker User Name is NOT NULL	This filter selects events in which the attacker user name field is populated.	Filter
Activity from Rogue Account IDs	This filter selects events where either the attacker or target user name is deemed to be a rogue account id. A rogue account ID is one that is unknown and cannot be associated to actors or other predefined accounts. Login attempts are excluded to eliminate false positives due to username typos.	Filter
Inbound Email	This filter selects events indicating email traffic from external domains to internal domains.	Filter
Physical Access System Events	This filter selects all events from physical access systems.	Filter
Actor Audit Events - Role Changes	This filter selects actor audit events generated by ESM when an actor resource's role attribute is updated.	Filter
No Actor with Authenticator	This filter identifies events where an authenticator can be derived from the event fields but an actor cannot.	Filter
ActorByAccountID is NULL	This filter selects events which can not be correlated to an actor based on the attacker or target user name fields.	Filter
ActorByAccountID is NOT NULL	This filter selects events which can be correlated to an actor based on the attacker or target user name fields.	Filter
Non-ArcSight Events	This filter selects events in which the Device Vendor and Device Product is not ArcSight.	Filter
Actor Audit Events - Actor Deleted by Interactive Session	This filter selects actor audit events generated by ESM when an actor resource is deleted by an interactive session. Its purpose is to find manual deletions made to actor resources.	Filter
User Privilege Added	This filter selects events indicating that new rights were assigned to a user.	Filter
Attacker User Name is NULL	This filter selects events in which the attacker user name field is not populated.	Filter
Event with User Name and without Actor	This filter identifies events that have a user name in them but cannot be attributed to an actor.	Filter
Actor Audit Events - Base Attribute Updated	This filter selects actor audit events generated by ESM when an actor's base attribute is updated.	Filter
ActorByIP is NOT NULL	This filter checks if an actor can be associated with the source IP address of the event.	Filter
Target User Name is NOT NULL	This filter selects events in which the attacker user name field is populated.	Filter

Resource	Description	Type
Arcsight Internal Events	This filter selects ArcSight ESM internally generated events.	Filter
Actor Audit Events - Role Added	This filter selects actor audit events generated by ESM when an actor resource's role attribute is added.	Filter
Actor Audit Events - Actor Added	This filter selects actor audit events generated by ESM when an actor resource is added.	Filter
Actor Audit Events - Role Deleted	This filter selects actor audit events generated by ESM when an actor resource's role attribute is deleted.	Filter
Actor Audit Events - Status Disabled	This filter selects actor audit events generated by ESM when an actor's base attribute is updated.	Filter
Actor Audit Events - Account Identifier Added	This filter selects actor audit events generated by ESM when an actor's account ID is added.	Filter
Attacker User Name is Rogue Account ID	This filter selects events where the attacker user name is unknown and cannot be associated to actors or other predefined accounts.	Filter
Email Traffic	This filter selects events indicating successful email communications.	Filter
Events without Actor	This filter identifies the events that cannot be attributed to an actor.	Filter
Events with Actor	This filter identifies events that can be attributed to an actor either by virtue of the event user name or the originating IP address.	Filter
Username Present	This filter checks whether any of attacker username, or target username are present in the event.	Filter
Target User Name is NULL	This filter selects events in which the target user name field is not populated.	Filter
Non-ArcSight Internal	This filter excludes internal ArcSight events.	Filter
Windows Events	This filter selects all events in which the device product field is Microsoft Windows.	Filter
Windows Exceptions for Target User Name Rogue Account ID checks	This filter identifies Microsoft Windows events that have a target user name which should not be attributed to a rogue account id.	Filter
Actor Audit Events	This filter selects all actor audit events generated by ESM when an actor resource is updated.	Filter
Actor Audit Events - Actor Deleted	This filter selects actor audit events generated by ESM when an actor resource is deleted.	Filter
Actor Attribute Modifications	This profile detects patterns of actor attribute modifications.	Profile
Actor Role Deletions	This profile detects patterns of actor role deletions.	Profile
Actor Role Additions	This profile detects patterns of actor role additions.	Profile

Resource	Description	Type
Top Applications with Activity from Rogue Account IDs	This query selects the top applications by count of the number of events that show activity attributable to rogue accounts IDs.	Query
Role Names	This query selects every role name and role type in the system, ordered by role name.	Query
Count of Roles by Type	This query selects the total number of actor role assignments per authenticator in the system.	Query
Actor Status Overview	This query selects each unique actor status value and the number of actors having that status.	Query
Top 20 Actors with Roles	This query selects the top actors by count of their role assignments.	Query
Number of Account IDs	This query selects the number of unique account IDs per authenticator in the system.	Query
Department Overview	This query selects the department from each actor, and counts the number of actors in that department.	Query
Actor Base Attributes	This query selects all single-value attributes (base attributes) for each actor in the system.	Query
Top 20 Entitled Actors for Department	This query selects the top actors from the specified department by count of their role assignments.	Query
Actors Status Disabled	This query selects information from actor audit events indicating an actor's status was set to disabled.	Query
Top 20 Roles	This query selects the top roles by count of the actors assigned to them.	Query
Actor Role Additions	This query selects actor audit events generated by ESM when an actor's role attribute is added.	Query
Top Target Addresses with Activity from Rogue Account IDs	This query selects the top target addresses by count of the number of events that show activity attributable to rogue accounts IDs.	Query
Leaf Node OUs	This query selects the leaf node organizational unit from actors distinguished names, and counts the number of actors in that organizational unit.	Query
Role Attestation for Actors with Specified Role	This query selects all role assignments for actors having the role specified when running the report.	Query
Roles by Actor	This query selects every actor's full name and roles.	Query
Activity from Rogue Account IDs - by Attacker User	This query selects the attacker user name, target host name, and count of events attributable to rogue accounts IDs, grouped by attacker user name and target host name.	Query
Actor All Attributes	This query on actors selects all attributes from each actor resource.	Query
Roles by Actor with Active Status	This query selects all roles for all actors who have a status of Active.	Query
Actor Role Deletions	This query selects actor audit events generated by ESM when an actor's role attribute is deleted.	Query

Resource	Description	Type
Number of Role Assignments	This query selects the total number of actor role assignments per authenticator in the system.	Query
Count of Roles by Memberships	This query on actors gives the number of actors that are assigned to each role.	Query
Actors with Specified Role	This query selects all role assignments for actors having the role specified when running the report.	Query
Actors Added	This query selects information from actor audit events indicating an actor resource was added to the system.	Query
Detailed Activity for Account ID	This query selects all activity that can be attributed to a single account id.	Query
Top Rogue Account IDs in Use	This query selects the top rogue account IDs by count of the number of events. Each rogue account ID is a combination of the attacker and target user names.	Query
Top Attacker Addresses with Activity from Rogue Account IDs	This query selects the top attacker addresses by count of the number of events that show activity attributable to rogue accounts IDs.	Query
Total Number of Actors	This query selects the number of unique actor resources in the system.	Query
Activity from Rogue Account IDs - by Target User	This query selects the target user name, target host name, and count of events attributable to rogue account IDs, grouped by target user name and host name.	Query
Rogue Account IDs	This query selects pertinent information from the Rogue Account IDs active list.	Query
Roles by Actor for Department	This query selects all roles for all actors in the specified department.	Query
IP Address to Actor Map	This session list tracks the IP addresses that can be associated with actors. Typically, these IP addresses will belong to single-user machines.	Session List

Actor Attribution by IP Address Use Case

The Actor Attribution by IP Address use case associates IP addresses to actors, and allows events from IP addresses to be attributed to the logged in actor, even if no username is present in the event.

In addition, the resources provided in the Actor Attribution by IP Address use case enable auditors, analysts, and managers to provide the following services:

- Actor attribution methods cover the following login scenarios:
  - **Single-user machine**—When an actor logs into a single-user machine, the machine's IP address is associated with actor indefinitely until another actor logs into the same single-user machine. All events that originate from that IP address during that time interval can be attributed to that actor.
  - **Server machine supporting multiple logins**—When an actor logs into a multi-user machine such as a server, these logins are tracked by default for 12 hours. Since multiple users might be logged in concurrently,

analysts can attribute events to the set of users who were logged in at a given time, but might not be able to identify the specific actor responsible for the event.

- Monitoring and reporting on server logins based on department, title, role, country or region, source zone, and actor status.
- Global variables that can be used by other resources to associate source and target IP addresses in events with actors. These global variables are used by other use cases.

The soInActorByTargetIP global variable provides the ability to attribute an actor to an event using the event's target IP address. The soInActorByTargetIP global variable (like the analogous source IP AsoInActorByTargetIP global variable) returns information about the actor such as the UUID, name, employee type, and title.

This use case provides resources that have been developed specially for the Microsoft Windows and UNIX operating systems. Microsoft Windows and UNIX specific configuration instructions are provided in Configure Resources. Please note the following:

- For single-user logins, Microsoft Windows Server 2003 is supported.
- For the server multi-user logins, both Microsoft Windows Server 2003 and Microsoft Windows Server 2008 are supported.

Categorize Assets and Zones

This use case requires categorization of assets and zones into the appropriate UBM Network Domains:

Single-user Machines—Classify the assets or zones that define the single-user machines into one of the following asset categories:

- ArcSight Solutions/UBM/Network Domains/Desktops
- ArcSight Solutions/UBM/Network Domains/Laptops

Server machine supporting multiple logins—Classify the assets or zones that define the server machines into the following asset category: ArcSight Solutions/UBM/Network Domains/Servers

The Source and Destination Subnets for Actor Logins query viewer shows source and destination sub-nets for actor login events. Use the results of this query viewer to determine the appropriate zones to create for your environment and to classify these zones into the appropriate single-user or server asset categories.

Devices

The following types of devices supply events to this use case:

- Operating System
- Intrusion Detection Systems/Intrusion Prevention System

- Identity Management

All the device types listed above can supply events to this use case but the resources will only process events from devices, when the device generates login events that can be attributed to specific actors.

Configure Resources

Configure the following types of resources for this use case:

- Active Lists
- Rules
- Filters

Some tuning of the default configuration might be required to eliminate false positives/negatives generated by this use case.

Active Lists

You might want to customize the following active lists for this use case:

- Populate the Account Exclusions active list with the account IDs which should not be considered when processing events to associate IP addresses to actors. All the entries must be in uppercase. If account ID is listed in the Account Exclusions active list, events associated with that account ID are not processed when associating IP addresses to actors.
- Populate the Excluded Source Machines active list with the source IP addresses which should not be considered when processing events to associate IP addresses to actors. If IP address is listed in the Excluded Source Machines active list, events associated with that IP address are not processed when associating IP addresses to actors.
- Populate the Excluded Target Machines active list with the target IP addressees which should **not** be considered when processing events to associate IP addresses to actors. If IP address is listed in the Excluded Target Machines active list, events associated with that IP address are not processed when associating IP addresses to actors.

Rules

Configure the following rules for this use case:

- Enable the Actor Logged Into Single-User Windows Machine rule, if you want to track all actor logins into Windows single-user machines. Before enabling the rule, verify that the ESM Manager is receiving events from a Microsoft Windows Server 2003 Domain Controller and that the Audit account logon events policy on the

Domain Controller is enabled for at least successful login attempts. After verifying the events, enable the rule. By default all the actions for this rule are enabled.

- Enable the Actor Logged into non-Windows Single-User Machine rule, if you want to track all actor logins into non-Windows single-user machines. By default all the actions for this rule are enabled.
- Enable the Actor Logged into non-Windows Server rule, if you want to track all actor logins into non-Windows server machines. By default all the actions for this rule are enabled.
- Enable the Actor Logged Into Windows Server rule if you want to track all actor logins into Microsoft Windows server machines. In addition, verify that the ESM Manager is receiving events from either a Microsoft Windows Server 2003 or Microsoft Windows Server 2008 Domain Controller and that the Audit logon events policy on the Domain Controller is enabled for successful login attempts. By default all the actions for this rule are enabled.

Session List

Configure the following session list for this use case:

Server Login Sessions—Server logins by specific actors are tracked in the Server Login Sessions session list. If an actor does not log in to a server for 12 hours, the entry for the actor/server combination is removed from the Server Login Sessions session list. You might want to adjust the time out period of the Server Login Sessions session list for your organization. You can change the default time-out period of 12 hours for the Server Login Sessions session list by editing the TTL Days value in the session list editor.

Filters

Verify that the following filters detect events in your environment that match the expected behavior for each filter:

- Actor Logged into Single-User Windows Machine
- Actor Logged into non-Windows Single User Machine
- Actor Logged into non-Windows Server
- Actor Logged into Windows Server

Verify Configuration

After configuring this use case, verify events are attributable to actors based on the originating IP address by viewing the Actor Changes active channel:

1. In the Navigator panel, go to Active Channels.
2. Navigate to ArcSight Solutions/UBM/Actor Attribution by IP Address.

3. Right-click All ActorAttribution by IP Address -Rule Firings and select **Show Active Channel**.All rule fire events for this use case should display.
4. Right-click Actor Changes and select Show Active Channel.

Only those events that can be attributable to actors based on the originating IP address should display.

Resources

The following table lists all the resources explicitly assigned to this use case and any dependent resources. Each resource can be accessed from the Actor Attribution by IP Address use case landing page: /All Use Cases/ArcSight Solutions/UBM/Actor Management, or their URI, for example: /All <Resource Type>/ArcSight Solutions/UBM/<Use Case>/<Resource Name>.

Resource	Description	Type
Monitor Resources		
Actor Logged into Server	This active channel shows actor login events to server machines.	Active Channel
Events with ActorByIP	This active channel shows all events that can be associated with an actor based on source IP address.	Active Channel
Login Events with ActorByIP	This active channel shows login events that can be associated with an actor, where the actor attribution is done using the source IP address.	Active Channel
All Actor Attribution by IP Address - Rule Firings	This active channel shows all correlation events for the Actor Attribution by IP Address use case.	Active Channel
Source and Destination Subnets for Actor Logins	This query viewer shows source and destination subnets for actor login events. Use the results of this query viewer to determine the appropriate zones to create for your environment and to classify these zones into the appropriate single-user or server asset categories.	Query Viewer
Actor Login Events	This query viewer displays login events that can be attributable to an actor using account IDs.	Query Viewer
Actors Currently Logged into Servers	This query viewer shows all actors that are currently logged into server machines.	Query Viewer
All Events for Actors Associated by Target IP Only	This query viewer shows all events that can be associated with an actor, where the actor attribution is done using the target IP address only.	Query Viewer
All Events for Actors Associated by Source IP Only	This query viewer shows all events that can be associated with an actor, where the actor attribution is done using the source IP address only.	Query Viewer
Current IP to Actor Associations	This query viewer returns details of current IP-to-actor associations within the given time frame.	Query Viewer
Actors Associated with a Workstation IP Address	This report shows details of all actors associated with a specific workstation (single-user machine) IP address within the given time frame.	Report

Resource	Description	Type
Server Logins by Country or Region	This report displays actor server logins by country or region.	Report
Server Logins by Department and Title	This report displays servers logged into for various actor department and title combinations.	Report
IP Associations for Actor	This query selects all the IP associations for an actor within the given time frame.	Report
Server Logins by Disabled Actors	This report displays all server logins that have been made by disabled actors.	Report
Server Logins by Actors with Common Roles	This report displays common roles across two or more actors that have logged into certain servers.	Report
Server Logins by Actors with Unique Roles	This report displays roles that are unique to only one actor that has logged into a certain server.	Report
Server Logins for Actor	This report shows information about server logins that can be attributed to a specific actor.	Report
All Actor to IP Associations	This report displays all IP-to-actor associations within the given time frame.	Report
Actors on Server	This report shows all actors that can potentially be associated with a server machine for the given time frame.	Report
Server Logins by Department and Source Zone	This report displays actor server logins by department and source zone.	Report
Library - Correlation Resources		
Actor Logged into Single-User Windows Machine	This rule triggers when it detects that an actor has logged into a Microsoft Windows single-user machine.	Rule
Actor Logged into Windows Server	This rule triggers when it detects that an actor has logged into a Microsoft Windows server machine.	Rule
Actor Logged into non-Windows Server	This rule triggers when an actor logs into a non-Microsoft Windows server machine.	Rule
Actor Logged into non-Windows Single-User Machine	This rule triggers when it detects that an actor has logged into a non-Microsoft Windows single-user machine.	Rule
Library Resources		
Account Exclusions	This active list maintains a list of account IDs, which when observed in an event, do not need to be considered when associating an IP address to an actor. All the entries must be in uppercase.	Active List
Excluded Source Machines	This active list maintains a list of source IP addresses, which when observed in an event, do not need to be considered when associating an IP address to an actor.	Active List

Resource	Description	Type
Account Authenticators	This active list is used by the actor global variables to determine what the Identity Management authenticator is, base on the event, so that an actor can be determined from event information.	Active List
Excluded Target Machines	This active list maintains a list of target IP addresses, which when observed in an event, do not need to be considered when associating an IP address to an actor.	Active List
Desktops	This is a solutions asset category.	Asset Category
Servers	This is a solutions asset category.	Asset Category
Laptops	This is a solutions asset category.	Asset Category
AttributableActor	This global variable returns all the information for an actor, where the event to actor attribution is done using either attacker or target user name fields, or the source IP address. Note: To turn lookups based on the source IP address, in the Parameters tab, do not use the actorByAccountOrSourceIP local variable to lookup the actor, use the UUID field of the ActorByAccountID global variable instead.	Global Variable
ActorByIP	This global variable returns all the information for an actor, where the event to actor attribution is done using the source IP address.	Global Variable
ActorByAccountID	This global variable maps the account information in an event with an actor. The account information consists of the device vendor and product, and information derived from the attacker or target user name, with preference to the target user name.	Global Variable
ActorFromIPMap	This global variable returns an actor's UUID, full name, username used, and login type if the actor is associated with a source IP address.	Global Variable
solnPatternDiscoveryConst	This variable returns a constant string that can be used in Pattern Discovery profiles when it is not required to specify either a Source or a Target event field.	Global Variable
solnActorByTargetIP	This global variable returns all the information about an actor, where the event to actor attribution is done using the target IP address.	Global Variable
AccountIDForLogins	This global variable determines which event username field to use.	Global Variable
ActorByUUID	This Actor global variable looks for a UUID in Device Custom String1, and retrieves the Actor with that UUID.	Global Variable
Actor Logged into Server	This field set selects the fields appropriate for viewing events that are associated with actor login events to server machines.	Field Set
Actor Attribution by IP Address - Rule Firings	This field set selects the fields appropriate for viewing correlation events for the Actor Attribution by IP Address use case.	Field Set
Events with ActorByIP	This field set selects the fields appropriate for viewing events that are associated with actors based on source IP address.	Field Set

Resource	Description	Type
Actor Logged into Single-User Windows Machine	This filter selects all actor login events to a Microsoft Windows single-user machines.	Filter
Successful Logins	This filter identifies successful logins by both administrative and non-administrative users across a variety of operating systems (Unix, Windows 2003, Windows 2008).	Filter
Target Username is a System Account	This filter selects events in which the target user name is a system account.	Filter
Successful Logins - Non-Windows and Non-Unix	This filter selects login events that cannot be attributed to either Microsoft Windows or Unix.	Filter
Attacker User Name is a System Account	This filter selects events in which the attacker user name is a system account.	Filter
Actor Activity on Server	This filter selects all actor activity to server machines.	Filter
Successful Logins - Windows 2003	This filter identifies successful login events to Windows 2003 domain controller machines.	Filter
Windows 2008 Authentication Ticket Request	This filter identifies Microsoft Windows 2008 events which indicate that a Kerberos authentication ticket was requested.	Filter
Actor not Associated with Source IP	This filter identifies events where an actor is not already associated with the incoming source IP. This filter is primarily used in the attribution rules.	Filter
Unix Events	This filter selects events that are coming from Unix devices.	Filter
Actor Logged into Windows Server	This filter identifies actor logins to Microsoft Windows server machines.	Filter
ActorByAccountID is NULL	This filter selects events which can not be correlated to an actor based on the attacker or target user name fields.	Filter
ActorByAccountID is NOT NULL	This filter selects events which can be correlated to an actor based on the attacker or target user name fields.	Filter
Windows 2003 Authentication Ticket Request	This filter identifies Microsoft Windows Kerberos Authentication Ticket Request events. These events are generated when a user logs into an Active Directory domain.	Filter
Target is Single-User Machine	This filter identifies events where the target machine is classified as a single-user machine.	Filter
Successful Logins - Windows 2008	This filter identifies successful login events to Windows 2008 domain controller machines.	Filter
Source is Single-User Machine	This filter identifies events where the source machine is classified as a single-user machine.	Filter

Resource	Description	Type
Machine and Account Exclusions	This filter combines the machine and account exclusions conditions.	Filter
Login Attempts	This filter selects any attempts at logging into systems. It excludes machine logins into Microsoft Windows systems.	Filter
Successful Logins - Unix	This filter identifies successful login attempts to Unix machines.	Filter
Server Login Rule Fire Events	This filter identifies all correlation events from rules monitoring logins to servers.	Filter
Windows Events with a Non-Machine User	This filters identified Microsoft Windows events that have a non machine/system user either in the attacker or the target fields.	Filter
Actor Associated with Source IP Only	This filter selects all events that can be associated with an actor, where the actor attribution is done using the source IP address.	Filter
Machine Exclusions	This filter selects all events which do not match the source IP addresses in either the Excluded Source Machines list or the target IP addresses in the Excluded Target Machines list.	Filter
Successful and Unsucessful Logins - Windows 2003	This filter identifies both successful and unsuccessful logins on Windows 2003 domain controller machines.	Filter
Username Present	This filter checks whether any of attacker username, or target username are present in the event.	Filter
Account Exclusions	This filter identifies all events which do not match the account IDs listed in the Account Exclusions list.	Filter
Actor Logged into non-Windows Server	This filter identifies actor login events to non-Microsoft Windows server machines.	Filter
Non-Windows Operating System Logins	This filter identifies login events to non-Microsoft Windows Operating Systems.	Filter
Actor Logged into non-Windows Single-User Machine	This filter selects all actor login events to a non-Microsoft Windows single-user machines.	Filter
Windows Events	This filter selects all events in which the device product field is Microsoft Windows.	Filter
Unsuccessful Logins for Valid Username - Windows 2003	This filter identifies unsuccessful logins for a valid username on Windows 2003 domain controller machines.	Filter
Actor Associated with Source IP or Username	This filter identifies events that have an actor associated with them, where the actor attribution is done using either account IDs or the source IP address.	Filter
Actor Associated with Target IP Only	This filter selects all events that can be associated with an actor, where the actor attribution is done using the target IP address.	Filter
Server Login Activity by Title and Department	This profile is used to detect patterns of server login activity across various actor title and department combinations.	Profile

Resource	Description	Type
Server Login Activity by Actors	This profile can be used to detect patterns of server login activity across actors.	Profile
All Events for Actors Associated by Target IP Only	This query selects all events that can be associated with an actor, where the actor attribution is done using the target IP address.	Query
Server Logins by Department and Source Zone	This query returns actor server logins by department and source zone.	Query
Server Logins by Disabled Actors	This query returns all server logins made by disabled actors.	Query
All Events for Actors Associated by Source IP Only	This query selects all events that can be associated with an actor, where the actor attribution is done using the source IP address.	Query
Source and Destination Subnets for Actor Logins	This query shows source and destination subnets for actor login events, where the actor attribution is done using account IDs. Data from this query can be used to determine how to create and classify asset zones into single-user or server asset categories.	Query
Server Logins by Department and Title	This query returns actor server logins by department and title.	Query
Actors Currently Logged into Servers	This query shows all actors that are currently logged into server machines.	Query
Actor Login Events	This query selects login events that can be associated with an actor, where the actor attribution is done using either the source or target user names.	Query
Actors on Server	This query selects all actors that can potentially be associated on a server machine for the given time frame.	Query
Current IP to Actor Associations	This query returns details of current IP-to-actor associations within the given time frame.	Query
Server Logins by Actors with Unique Roles	This query selects roles that are unique to only one actor that has logged into a certain server.	Query
Server Logins for Actor	This query shows information about server logins that can be attributed to a certain actor.	Query
Server Logins by Actors with Common Roles	This query shows common roles across two or more actors that have logged into certain servers.	Query
Server Logins by Country or Region	This query returns actor server logins by country or region.	Query
All IP to Actor associations	This query selects all IP-to-actor associations within the given time frame.	Query
IP Associations for Actor	This query selects all the IP associations for an actor within the given time frame.	Query

Resource	Description	Type
Actors Associated with an IP Address	This query returns details of all actors associated with a specific IP address within the given time frame.	Query
IP Address to Actor Map	This session list tracks the IP addresses that can be associated with actors. Typically, these IP addresses will belong to single-user machines.	Session List
Server Login Sessions	This session list keeps track of all actor logins into server machines. The list has a default expiration time of 12 hours.	Session List

Shared Accounts Use Case

The Shared Accounts use case reports on the usage of accounts that might be in use by more than one individual. The use case can detect when anyone uses an existing known shared account, as well as detect the use of any account by more than one individual.

In addition, the resources contained in the Shared Accounts use case enables auditors, analysts, and managers to provide the following services:

- Report on the logins to known and detected shared accounts
- Report on actors who use shared accounts
- Report on the IP addresses of machines that are being accessed by shared accounts
- Report on the applications that are being accessed by shared accounts
- Report on the account IDs that are using shared accounts
- Report on actors who log in from two different countries within a short time period
- Report on the departments, job titles, and roles associated with actors using accounts known to be shared or accounts detected to be shared
- Detect patterns of activity that might indicate the use of new shared accounts (not previously known)
- Detect patterns of activity across the usage of shared accounts

The use case reports actors that have used known shared accounts. When an event is collected that indicates a known shared account has been used, the actor attributable to the event is determined in one of the following ways:

- The account ID listed in the login event (Actor By Name)
- The originating IP address (Actor By IP)

UBM recommends that this use case be used in conjunction with the Actor Attribution by IP Address Use Case. Configuring the Actor Attribution by IP Address Use Case provides better reporting on the actors using shared accounts. Many login events do not contain enough information to determine the actor associated with an event

from the username but the Actor Attribution by IP Address Use Case provides functionality to determine the associated actor from the originating IP address. For more information, see Actor Attribution by IP Address Use Case.

Devices

All the devices that report logins can supply events to this use case but the resources will only process events from devices, when the device generates events that can be attributed to specific actors.

Configure the Windows Audit Policy

To enable this detection on Microsoft Windows operating systems, please configure the following audit policies:

- **For Windows 2003 and earlier**—The Audit logon events and Audit account logon events policies must be enabled for both successful and failed login attempts.
- **For Windows 2008 and Newer**—The Audit logon events policy must be enabled for both successful and failed login attempts.

For more information about enabling policies, see your Microsoft Windows operating system documentation.

Configure Resources

Configure the following types of resources for this use case:

- Active Lists
- Filters
- Rules

Active Lists

The following active lists might need to be configured for this use case:

- Review the Known Shared Accounts active list and add any additional known shared accounts that you want to monitor. Remove existing entries from the list if they are not applicable to your environment, or if you do not want to receive reports on how or when those entries are used. Note that the Account IDs specified in the active list must be in uppercase and the Applications specified in the active list must match the Device Product field of the events.
- You might want to periodically maintain the Detected Shared Accounts active list. When the Record Account IDs in Use rule detects an account ID is first used by any actor, the rule stores the account ID and associated actor in the Account IDs in Use active list. When the Detect Shared Accounts rule detects that another actor is using the same account ID, it adds an entries for both actors into the Detected Shared Accounts active list. To report on

detected shared accounts, the Detected Shared Accountsactive list is queried by the output resources such as reports, query viewers and dashboards.

- Use the Actor Logins to Detected Shared Accounts report, to investigate a potential set of login events that cause accounts to be detected as shared. At some point, you might want to stop reporting these account IDs as detected shared accounts and instead report them as known shared accounts. To do this remove the entries for the account ID from the Detected Shared Accounts active list and add them to the Known Shared Accounts active list.
- All actor/account associations are tracked in the Account IDs in Use active list, so the Account IDs in Use active list grows to contain many entries. If an actor does not use an account for 90 days, the entry for the actor/account association is removed from the Account IDs in Use active list. You might want to adjust the time out period of the Account IDs in Use active list for your organization. You can change the default time-out period of 90 days on the Account IDs in Use active list by editing the TTL Days value in the active list editor.

Filters

Verify that the following filters detect events in your environment that match the expected behavior for each filter:

- All Login Events to Known Shared Accounts
- Failed Logins to Known Shared Accounts

Rules

Enable the following rules if you want to detect when an account ID is being used by two or more actors:

Enable the Record Account IDs in Use rule. By default the rule invokes the following action:

- **Set Event Field Actions**—Sets the agent severity to medium for the event generated by this rule and attempts to attribute the event to an actor by invoking the ActorByIPOrAccount global variable.

Enable the Detect Shared Accounts rule to detect new shared accounts. By default the rule invokes the following actions:

- **Set Event Field Actions**—Sets the agent severity to medium for the event generated by this rule and attempts to attribute the event to an actor by invoking the ActorByIPOrAcount global variable.
- **Add to Active List**—Adds an entry to the Detect Shared Accounts active list, which contains the first actor detected using a shared account, the account ID, UUID and associated application.

By default, the following action of the Detect Shared Accounts rule is disabled. You can optionally enable this action:

- **Add to Existing Case—**Adds a case to the specified URI.

The following rules can be configured for this use case:

Enable the Login to Shared Account By Actor rule if you want to track the logins into known shared accounts. If this rule is enabled and this activity is detected, by default the rule invokes the following action:

- **Set Event Field Actions**—Sets the agent severity to medium for the event generated by this rule and attempts to attribute the event to an actor by invoking the AttributableActor global variable.

Enable the Actor Logged in from Two Countries rule if you want to track when an actor has logged in from two countries during a short time period. By default, the following action of the Actor Logged in from Two Countries rule is disabled. You can optionally enable these actions:

- **Add to Existing Case**—Adds a case to the specified URI. For more information, see
- **Set Event Field Actions**—Sets the agent severity to high for the event generated by this rule and attempts to attribute the event to an actor by invoking the ActorByAccountID global variable.

You might want to also adjust the time frame (in the Aggregation tab) to reflect an appropriate time period for your environment.

Verify Configuration

After configuring this use case, you can check on shared account usage by viewing the following dashboards:

Detect Shared Accounts

Known Shared Account Logins

Known Shared Account Usage

To view a dashboard:

1. In the Navigator panel, go to **Dashboards**.
2. Navigate to ArcSight Solutions/UBM/Shared Accounts.
3. Right-click the dashboard and select **Show Dashboard**.

Depending on the dashboard opened, any detected or known shared accounts will display.

Resources

The following table lists all the resources explicitly assigned to this use case and any dependent resources. Each resource can be accessed from the Shared Accounts use case landing page: /All Use Cases/ArcSight Solutions/UBM/Actor Management, or their URI, for example: /All <Resource Type>/ArcSight Solutions/UBM/<Use Case>/<Resource Name>.

Resource	Description	Type
Monitor Resources		
Logins to Known Shared Accounts	This active channel shows rule trigger events associated with logins to known shared accounts.	Active Channel
Known Shared Account Logins	This dashboard shows information about the top applications and addresses that are associated with logins to known shared accounts.	Dashboard
Known Shared Account Usage	This dashboard displays statistical information about how known shared accounts are being used.	Dashboard
Detected Shared Accounts	This dashboard displays statistical information about detected shared accounts.	Dashboard
Top Actors by IP Using Known Shared Accounts	This query viewer returns the top actors that have been identified by a source IP address which are using known shared accounts to log in.	Query Viewer
Top Applications with Known Shared Account Logins	This query viewer returns the top applications using known shared accounts within the last two hours.	Query Viewer
Top Actors Using Detected Shared Accounts	This query viewer returns the top actors detected as using shared accounts.	Query Viewer
Top Detected Shared Accounts	This query viewer returns the top detected shared accounts and their associated applications.	Query Viewer
Top Target Addresses with Known Shared Account Logins	This query viewer returns the top target addresses involved in login events to known shared accounts that have occurred within the last two hours.	Query Viewer
Top Actors by Name Using Known Shared Accounts	This query viewer shows the top actors that can be identified by the Attacker User Name field and that are using known shared accounts to log in.	Query Viewer
Top Applications with Detected Shared Accounts	This query viewer returns the top applications associated with accounts detected as shared.	Query Viewer
Actors Logged in from Two Countries	This query viewer shows those actors that have logged in from two countries within a short time interval.	Query Viewer
Top Known Shared Accounts in Use	This query viewer shows the number of times each known shared account has been used in login events.	Query Viewer
Recent Logins to Known Shared Accounts	This query viewer shows details about recent login events to known shared accounts.	Query Viewer
Top Source Addresses with Known Shared Account Logins	This query viewer returns the top source addresses associated with login events to known shared accounts that have occurred within the last two hours.	Query Viewer
Detected Shared Accounts	This report returns the details of accounts that have been identified as being shared by two or more actors.	Report

Resource	Description	Type
Top Roles Using Shared Accounts	This report shows the top roles by number of actors that have been identified as using shared accounts.	Report
Top Departments Using Shared Accounts	This report shows the top departments by number of actors that have been identified as using shared accounts.	Report
Top Job Titles Using Shared Accounts	This report shows the top job titles by number of actors that have been identified as using shared accounts.	Report
Logins to Known Shared Accounts - Details	This report shows details of all login events to known shared accounts.	Report
Logins to Known Shared Accounts - Summary	This report shows summary information about logins to known shared accounts.	Report
Actor Logins to Detected Shared Accounts	This report shows details of actor login events to accounts that have been detected as being shared.	Report
Library - Correlation Resources		
Record Account IDs in Use	This rule triggers when it identifies login events from which an association that has not been previously recorded can be made between an actor and a username. The rule records this association in the Account IDs in Use active list.	Rule
Actor Logged in from Two Countries	This rule detects if an actor has logged in from two different countries within a short time period. This might indicate either that the actor's account ID has been compromised or that the account ID is being shared.	Rule
Login to Known Shared Account by Actor	This rule triggers on login events to known shared accounts.	Rule
Detect Shared Accounts	This rule triggers when it discovers that a single username is being used by one or more actors.	Rule
Library Resources		
Account IDs in Use	This active list keeps track of all the account IDs that are being used by all actors. Entries are expired every 90 days to prevent the list from becoming too large.	Active List
Detected Shared Accounts	This active list is populated when an account and application combination is detected to be shared between one or more actors.	Active List
Account Authenticators	This active list is used by the actor global variables to determine what the Identity Management authenticator is, base on the event, so that an actor can be determined from event information.	Active List
Known Shared Accounts	This active list maintains a list of known shared accounts per application. Note that all account IDs must be in uppercase and the Application field must be the same as what appears in the Device Product event field.	Active List
Failed Logins to Known Shared Accounts by Application	This data monitor shows a moving average of failed logins to known shared accounts per application.	Data Monitor

Resource	Description	Type
AttributableActor	This global variable returns all the information for an actor, where the event to actor attribution is done using either attacker or target user name fields, or the source IP address. Note: To turn lookups based on the source IP address, in the Parameters tab, do not use the actorByAccountOrSourceIP local variable to lookup the actor, use the UUID field of the ActorByAccountID global variable instead.	Global Variable
ActorByIP	This global variable returns all the information for an actor, where the event to actor attribution is done using the source IP address.	Global Variable
ActorByAccountID	This global variable maps the account information in an event with an actor. The account information consists of the device vendor and product, and information derived from the attacker or target user name, with preference to the target user name.	Global Variable
ActorFromIPMap	This global variable returns an actor's UUID, full name, username used, and login type if the actor is associated with a source IP address.	Global Variable
ActorByIPOrAccount	This global variable attempts to attribute an actor to an event based on source IP or account (in that order).	Global Variable
solnPatternDiscoveryConst	This variable returns a constant string that can be used in Pattern Discovery profiles when it is not required to specify either a Source or a Target event field.	Global Variable
ActorByAttackerUserName	This variable maps the account information in an event with an actor. The account information consists of the device vendor, device product, connector address, connector zone, and information derived from the attacker user name.	Global Variable
AccountIDForLogins	This global variable determines which event username field to use.	Global Variable
ActorByUUID	This Actor global variable looks for a UUID in Device Custom String1, and retrieves the Actor with that UUID.	Global Variable
Events with AttributableActor	This field set selects the fields appropriate for viewing events correlated with either account-id or IP address and can be customized for the UBM active channels.	Field Set
Shared Account Login Events	This field set selects the fields appropriate for viewing login events to shared accounts.	Field Set
Logins to Accounts not Known to be Shared from non-IDS Devices	This filter selects login events to accounts that are not classified as Known Shared Accounts and are from non-IDS type devices.	Filter
Target Username is a System Account	This filter selects events in which the target user name is a system account.	Filter
Successful Logins	This filter identifies successful logins by both administrative and non-administrative users across a variety of operating systems (Unix, Windows 2003, Windows 2008).	Filter
ActorByAttackerUserName is NULL	This filter selects events which cannot be attributed to an actor based on the attacker user name field.	Filter

Resource	Description	Type
Attacker User Name is a System Account	This filter selects events in which the attacker user name is a system account.	Filter
Successful Logins - Windows 2003	This filter identifies successful login events to Windows 2003 domain controller machines.	Filter
Attacker User Name is NOT NULL	This filter selects events in which the attacker user name field is populated.	Filter
Windows 2008 Authentication Ticket Request	This filter identifies Microsoft Windows 2008 events which indicate that a Kerberos authentication ticket was requested.	Filter
ActorByAccountID is NULL	This filter selects events which can not be correlated to an actor based on the attacker or target user name fields.	Filter
Failed Logins to Known Shared Accounts	This filter identifies failed logins to known shared accounts.	Filter
ActorByAccountID is NOT NULL	This filter selects events which can be correlated to an actor based on the attacker or target user name fields.	Filter
Attributable Actor is NOT NULL	This filter selects events in which an actor can be attributed to an event either by username or by source IP.	Filter
Windows 2003 Authentication Ticket Request	This filter identifies Microsoft Windows Kerberos Authentication Ticket Request events. These events are generated when a user logs into an Active Directory domain.	Filter
Address or Username Present	This filter checks whether any of attacker address, attacker username, or target username are present in the event.	Filter
Record Account ID in Use	This file identifies login events from which an association that has not been previously recorded can be made between an actor and a username.	Filter
ActorByIP is NOT NULL	This filter checks if an actor can be associated with the source IP address of the event.	Filter
Shared Account Detector - Pattern Discovery	This filter identifies events to be processed by the Shared Account Detector pattern discovery profile.	Filter
Login Attempts	This filter selects any attempts at logging into systems. It excludes machine logins into Microsoft Windows systems.	Filter
Successful Logins - Unix	This filter identifies successful login attempts to Unix machines.	Filter
All Login Events to Known Shared Accounts	This filter identifies all login events in which a known shared account is being used. For this filter to work correctly, the Known Shared Accounts active list must be populated with all known shared accounts and their associated applications. This filter will identify successful, failed, and attempted logins.	Filter
Windows Events with a Non-Machine User	This filters identified Microsoft Windows events that have a non machine/system user either in the attacker or the target fields.	Filter

Resource	Description	Type
ActorByAttackerUserName is NOT NULL	This filter selects events in which the attacker user name field is populated, and the event can be attributed to an actor based on that field.	Filter
Unsuccessful Windows Logins for Valid Username	This filter identifies unsuccessful login events for a valid username recorded on Microsoft Windows domain controllers.	Filter
Successful and Unsucessful Logins - Windows 2003	This filter identifies both successful and unsuccessful logins on Windows 2003 domain controller machines.	Filter
Username Present	This filter checks whether any of attacker username, or target username are present in the event.	Filter
Unsuccessful Logins for Valid Username - Windows 2008	This filter identifies unsuccessful logins for a valid username on Windows 2008 domain controller machines.	Filter
Attributable Actor is NULL	This filter selects events which can not be correlated to an actor based on the attacker or target user name fields, or by the attacker address field.	Filter
Windows Events	This filter selects all events in which the device product field is Microsoft Windows.	Filter
Unsuccessful Logins for Valid Username - Windows 2003	This filter identifies unsuccessful logins for a valid username on Windows 2003 domain controller machines.	Filter
Actor Associated with Source IP or Username	This filter identifies events that have an actor associated with them, where the actor attribution is done using either account IDs or the source IP address.	Filter
Activity Across Known or Detected Shared Accounts	This filter identifies events where either a known or detected shared account is being used. Login events are excluded so as to determine other activity performed using shared accounts.	Filter
Unsuccessful or Attempted Logins	This filter identifies all login events in which the outcome was not a definite success, in other words either a failure or an attempt.	Filter
Shared Account Detector	This pattern discovery profile identifies patterns in user login activity. By default, patterns will be identified when the same set of one or more account IDs are accessed from two or more different source addresses. This might assist in the identification of shared accounts. This profile processes successful login events.	Profile
Activity Across Shared Accounts	This pattern discovery profile identifies patterns of activity across events where a shared account is used. Login events are excluded to determine other activity performed using shared accounts.	Profile
Top Roles Using Known Shared Accounts - Actor by IP	This query returns the top roles by number of actors that are using known shared accounts to log in. The actors in this query are identified by the event source IP address. Only those roles that have are detected across two or more actors are selected.	Query
Top Roles Using Detected Shared Accounts	This query returns the top roles by number of actors that have been detected as using shared accounts. Only those roles that have are detected across two or more actors are selected.	Query
Top Source Addresses with Known Shared Account Logins	This query returns the top source addresses associated with login attempts to known shared accounts.	Query

Resource	Description	Type
Top Job Titles Using Known Shared Accounts - Actor by IP	This query returns the top job titles by number of actors that are using known shared accounts to log in. The actors in this query are identified by the event source IP address.	Query
Top Detected Shared Accounts	This query returns the top detected shared accounts and their associated applications.	Query
Top Departments Using Known Shared Accounts - Actor by IP	This query returns the top departments by number of actors that are using known shared accounts to log in. The actors in this query are identified by the event source IP address.	Query
Top Job Titles Using Detected Shared Accounts	This query returns the top job titles by number of actors that have been detected as using shared accounts.	Query
Detected Shared Accounts	This query returns details of accounts that have been identified as being shared by two or more actors.	Query
Actors Logged in from Two Countries	This query identifies rules that triggered because an actor logged in from two countries within a short time interval.	Query
Logins to Known Shared Accounts - Details	This query retrieves the details of each event associated with a login to a known shared account.	Query
Top Departments Using Detected Shared Accounts	This query returns the top departments by number of actors that have been detected as using shared accounts.	Query
Top Roles Using Known Shared Accounts - Actor by Name	This query returns the top roles by number of actors that are using known shared accounts to log in. The actors in this query are identified by the Attacker User Name field. Only those roles that have are detected across two or more actors are selected.	Query
Actor Logins to Detected Shared Accounts	This query extracts details of actor login events to accounts that have been detected as being shared.	Query
Top Actors Using Detected Shared Accounts	This query returns the top actors detected as using shared accounts.	Query
Top Target Addresses with Known Shared Account Logins	This query returns the top target addresses involved in login attempts to known shared accounts.	Query
Top Applications With Known Shared Account Logins	This query returns the top applications using known shared accounts.	Query
Top Departments Using Known Shared Accounts - Actor by Name	This query returns the top departments by number of actors that are using known shared accounts to log in. The actors in this query are identified by the Attacker User Name field.	Query
Top Actors by Attacker User Name Using Known Shared Accounts	This query returns the top actors that can be identified by the Attacker User Name field and that are using known shared accounts to log in.	Query

Resource	Description	Type
Top Actors by IP Using Known Shared Accounts	This query returns the top actors identified by a source IP address that are using known shared accounts to log in.	Query
Top Job Titles Using Known Shared Accounts - Actor by Name	This query returns the top job titles by number of actors that are using known shared accounts to log in. The actors in this query are identified by the Attacker User Name field.	Query
Known Shared Account Usage	This query returns the number of times each known shared account and application combination has been used in login events.	Query
Top Applications with Detected Shared Accounts	This query returns the top applications associated with accounts detected as shared.	Query
IP Address to Actor Map	This session list tracks the IP addresses that can be associated with actors. Typically, these IP addresses will belong to single-user machines.	Session List

Actor Threat Score Use Case

The Actor Threat Score use case provides a method for tracking the level of suspicious activity exhibited by monitored users. Analysts are notified when an actor's suspicious activity exceeds configurable levels. Actors with high threat scores are monitored at a higher level of scrutiny.

This use case also provides:

- Reports and query viewers that provide additional visibility into the aggregate threat score by department, job title, and country.
- A dashboard and query viewers that show the top activity that increases threat scores.
- The new dashboard, reports and query viewers are based on the following trends:
  - Threat Score Contributors
  - Weekly Department Threat Score
  - Rules that detect and report on manual changes to the Actor Changes active list such as the removal of actors from the list or when the threat score associated with an actor is reduced.

The UBM solution tracks the suspicious behavior of actors using a threat score. The rules provided in the Suspicious Activity Use Case increase the threat score associated with each actor. These threat scores are used by the Actor Threat Score Use Case to report on the suspicious activities of actors.

The cumulative threat score associated with an actor reflects all the suspicious activity associated with all accounts attributed that specific individual, not just the behavior of a single account. For example, if suspicious activity for Jane Doe has already been detected for Jane Doe’s database account resulting in a current threat score of 15, when it is detected that Jane Doe’s Windows account clears an audit log, 5 more points are added to the threat score resulting in a cumulative threat score of 20. When the threat score for an actor reaches 30, the actor is considered

malicious. If the Actor Changes rule is enabled and configured, a notification is sent to an analyst and a case is created when an actor's threat score reaches 30.

The Suspicious Activity Use Case rules feed the threat score of actors. These rules determine the actor attributable to an event, using a global variable.

Each suspicious activity rule takes the actor's UUID and full name returned from the global variable and populates the following event fields in the generated correlation event:

`deviceCustomString1` field with the UUID

`deviceCustomString2` field with full name of the actor

Regardless of which global variable the rule invokes to get the attributable actor, the UUID (Universally Unique Identifier) and full name are always placed into the same Device Custom Strings fields of the generated correlation event. The values in the `deviceCustomString1` and `deviceCustomString2` are available for consumption by the Actor Threat Score Use Case resources. For example, the Threat Score Rule Firings for Actors on the Threat Score List query invokes the ActorByUUID global variable to determine the events associated with actors with suspicious behavior. The ActorByUUID global variable uses the UUID stored in `deviceCustomString1` and returns the actor associated with that UUID.

The UUID is the Universally Unique Identifier for the actor assigned by the Identity Management System. The UUID is the Universally Unique Identifier for the actor assigned by the Identity Management System.

The generated correlation event is populated with an agent severity that corresponds to the threat score associated with rule as specified in the following table. The value to add to the existing actor's threat score for a specific suspicious activity is stored in the Increase Actor Threat Score active list.

Association Between Agent Severity and Threat Score Increase

Agent Severity	Threat Score Increase	Result of Rule Trigger
Medium	+1	When a rule with a agent severity of medium is triggered, the rule adds +1 to the threat score of the actor attributed to generating the event.
High	+5	When a rule with a agent severity of high is triggered, the rule adds +5 to the threat score of the actor attributed to generating the event.
Very High	+25	When a rule with a agent severity of very high is triggered, the rule adds +25 to the threat score of the actor attributed to generating the event.

The relationship between the Agent Severity and the Threat Score is by convention only.

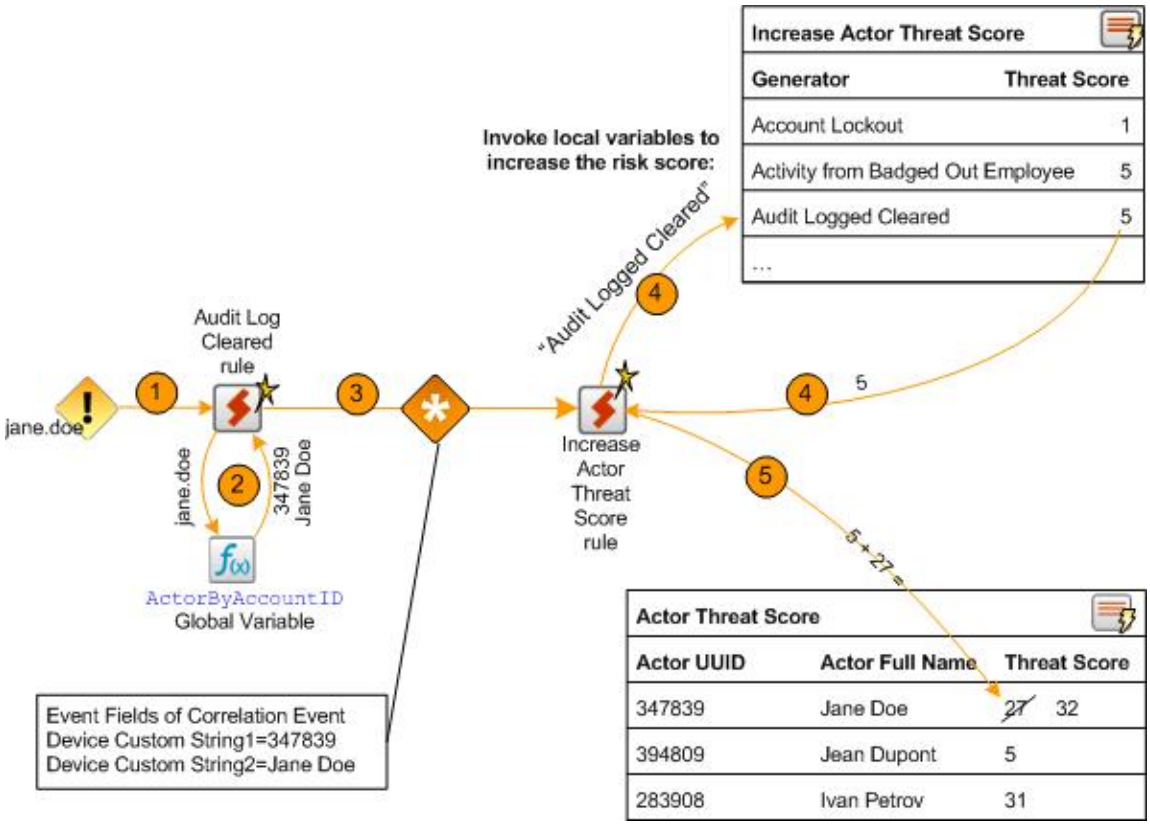
The Increase Actor Threat Score active list contains the suspicious activity rules that trigger an increase to the threat score and the values that should be added to the actor's threat score when that suspicious behavior is detected.

The suspicious activity rules generate correlation events and these correlation events trigger the Increase Actor Threat Score and Add Actor to Threat Score List rules:

- The first time suspicious activity is detected for an actor, the Add Actor to Threat Score List rule creates a new entry for the actor in the Actor Threat Score active list. It sets the actor's threat score in the active list to the threat value associated with the suspicious activity.
- If suspicious activity has already been detected for an actor, the Increase Actor Threat Score rule adds the threat score associated with the new suspicious activity to the existing threat score associated with an actor and updates the threat score associated with the actor in the Actor Threat Score active list.

The threat score associated with an actor is cumulative and by default always increases. An actor does not age off the Actor Threat Score active list. You can however, manually edit the threat score for an actor. For example, if you have investigated an actor and determined that his behavior is not malicious, you can lower his threat score manually, or remove the actor and threat score from the active list. (For more information, see Customizing the Threat Score Associated with a Suspicious Activity—Optional.) Once the threat score of an actor reaches 500, the Actor Changes rule stops firing and the threat score for the actor stops increasing.

Threat Score Mechanics



The following steps show an example of how suspicious activity is detected and processed by a rule in the Suspicious Activity Use Case. The steps listed below correspond to the orange numbered arrows located at the top of Threat Score Mechanics:

1. One of the suspicious activity rules is triggered. In this example, the AuditLogCleared s rule is triggered when an event indicating an audit log has been detected.
2. When the rule is triggered, it invokes either an ActorByX global variable or the AttributableActor global variable to determine the UUID associated with the triggering event, where X is the event field used to determine the UUID. The UUID is a unique identifier that is used as a key to an actor. For example, the AuditLogChanges rule invokes the ActorByAccountID global variable to determine the UUID associated with the Account ID of the triggering event.
3. The suspicious activity rule generates a correlation event. The suspicious activity rule populates the following fields in the correlation event:

- `deviceCustomString1` field with the UUID
- `deviceCustomString2` field with full name of the actor

In this example, a correlation event is generated by the Audit Log Cleared rule.

4. Because the actor who generated the event already has a threat score, the Increase Actor Threat Score triggers.
5. The rule action takes the new threat score associated with the UUID and updates the Actor Changes active list.

Threat Score Associated with Suspicious Rules and Stored in the Active List

Suspicious Activity Rule	Threat Score
Account Lockout	1
Activity from Badged Out Employee	5
Activity from Disabled Actor	5
Actor Added and Removed From Privileged Group Within a Short Time	5
After Hours Building Access by At Risk Actor	1
After Hours Database Access by At Risk Actor	5
Anonymous Proxy Access	25
Audit Log Cleared	5
Compromise - Attempt	5
Each resource can be accessed from the Actor Management use case landing page	1

Suspicious Activity Rule	Threat Score
Consecutive Unsuccessful Logins to Same Actor from different IPs	1
Data Manipulated	1
Database Brute Force Login Success	25
Default Vendor Account Attempt	5
Excessive Printing	1
Failed Building Access	5
Golden Ticket Attack Detected	25
Hacker Tool Website Access	5
IPC Share Browsing	1
Job Hunting	1
Large Email to Competition	5
Large Email to Public Webmail Servers	1
Leak of Company Information	5
Leak of Personal Information	5
Local Admin Created	1
Login to Known Shared Account by Actor	1
Multiple Failed Database Access Attempts	5
Multiple MITRE Techniques Against the Same Actor	25
Multiple Systems Logged into by Same User in a Short Time	10
Network Scan	5
Non-DBA Added to Oracle DBA Role	5
Pass-the-Hash Attack Detected	25
Physical Plus VPN Access	5
Possible Automated collection via PowerShell	5
Possible Data Exfiltration	5
Possible Data Exfiltration to External Website via PowerShell	5
Possible Data Theft Through Removable Media from the Same Machine	5

Suspicious Activity Rule	Threat Score
Possible LSASS Memory Dumping	25
Possible Scrapping of Outlook Inbox via PowerShell	5
Potential Data Theft Through Removable Media across Multiple Machines	25
Printing After Hours	1
Printing Confidential Documents	5
Printing Suspicious Documents	5
Resume Emailed by At Risk Actor	1
Role Violation	1
Security Software Disabled	25
Silver Ticket Attack Detected	25
Successful Brute Force Account Login	15
Suspicious Activity by Privileged Actor	5
Traffic to Competition	1
Traffic to Country of Concern	1
Using Different Usernames	1
VPN Login from Competition Domain	5

Devices

The following types of devices supply events to this use case:

- Security Information Event Management (SIEM) devices
- Devices listed in the Suspicious Activity Use Case, see Devices

Configure Resources

This use case requires that the desired Suspicious Activity Use Case rules are deployed and enabled. The Actor Threat Score Use Case rules update threat scores of actors when the Suspicious Activity Use Case rule fire.

Configure the following types of resources for this use case:

- Rules
- Filters

- Trends

In addition, consider the following optional configurations for this use case:

Manually Adjusting the Threat Score—Optional

Aging Actors Off the Actor Threat Score Active List—Optional

Customizing the Threat Score Associated with a Suspicious Activity—Optional

Adding Your Suspicious Activity Rules—Optional

Rules

The following rules can be configured for this use case:

Enable the Increase Actor Threat Score rule. **This rule is the foundation of this use case and must be enabled**.

By default, all the following actions of this rule are enabled:

- **Add to Active List**—Updates the existing actor's threat score by adding the threat value associated with the suspicious activity to the existing threat score and saves the new value into the existing entry for that actor in the Actor Threat Score active list.
- **Set Event Field Actions**—Sets field values for the event generated by this rule.

Enable the Add Actor to Actor Threat Score List rule. This rule is the foundation of this use case and must be enabled.

By default, all the following actions of this rule are enabled:

- **Add to Active List**—Adds the actor to the Actor Threat Score active list and sets the actor's threat score to the threat value associated with the suspicious activity.
- **Set Event Field Actions**—Sets field values for the event generated by this rule.

Enable the Actor Removed from Actor Threat Score rule if you want to track when ESM users remove an actor from the Actor Threat Score active list.

By default, the following action of this rule is enabled:

- **Set Event Field Actions**—Sets field values for the event generated by this rule.

By default, the following actions of the Actor Removed from Actor Threat Score rule are disabled. You can optionally enable these actions:

Send Notification—Sendsa notification to the destinations configured in the CERT Team. For more information, .

Add to Existing Case—Adds a case to the specified URI. For more information, see .

You can add exclusions to the filter referenced by this rule, to prevent this rule from firing for specific ESM users. For more information, see Filters.

Enable the Actor Changes rule if you want to track when the behavior of an individual is considered to be malicious because a threat score greater than 29 is associated with the actor. If this rule is enabled and this activity is detected, by default the rule invokes the following action:

- **Send Notification**—Sendsa notification to the destinations configured in the CERT Team.

By default, the following action of the Actor Removed from Actor Threat Score rule is disabled. You can optionally enable this action:

- **Add to Existing Case**—Adds a case to the specified URI.

Enable the Actors Removed from Actor Threat Score rule if you want to track when ESM users reduce a threat score in the Actor Threat Score active list.

By default, the following action of this rule is enabled:

- **Set Event Field Actions**—Sets field values for the event generated by this rule.

By default, the following actions of the Actor Removed from Threat Score List rule are disabled. You can optionally enable these actions:

- **Send Notification**—Sendsa notification to the destinations configured in the CERT Team.
- **Add to Existing Case**—Adds a case to the specified URI.

You can add exclusions to the filter reference by this rule, to prevent this rule from firing for specific ESM users. For more information, see Filters.

Filters

The following filters can be configured for this use case:

- Customize the following filters to exclude events for the set of ESM users who are expected to remove or change the threat scores in the Actor Threat Score active list:
- The Actor Threat Score Reduced rule references the Actor Threat Score Updated filter to determine the events processed by the rule.
- The Actor Removed from Actor Threat Score List rule references the Deleted Entry from Actor Threat Score List filter to determine the events processed by the rule.

For example, if the ESM user called admin is expected to remove or change the threat scores in the Actor Threat Score active list, add a condition to the filters to exclude audit events generated by that ESM user.

Trends

Reports and query viewers in this use case are based on the trends listed below. Before enabling these trends, verify that these trends collect the expected events for your environment. In addition, you might want to customize the trend before enabling. For more information, see .

Enable the following trends for this use case:

- Threat Score Contributors
- Weekly Department Threat Score

Manually Adjusting the Threat Score—Optional

The Actor Threat Score active list contains the actors which have been linked to suspicious activity and their associated threat score. This active list is dynamically populated by the Increase Actor Threat Score rule when suspicious events are detected. You might however, want to manually initially populate with some actors and threat scores or adjust the threat score associated with an actor.

To customize a threat score of an actor in the Actor Threat Score active list:

1. In the Navigator panel, select the Resources tab and the **Lists** option.
2. Expand the ArcSight Solutions/UBM/Actor Threat Score group.
3. Right-click the Actor Threat Score active list and select **Show Entries**.
4. Change, add or delete entries:

- Change an existing threat score. Right-click an entry in the Viewer and select **Edit**.
- To add an actor—Click the **Add Entry** () icon.
- To delete an actor—Right-click an entry in the Viewer and select **Delete**.

Aging Actors Off the Actor Threat Score Active List—Optional

By default, actors stay on the Actor Threat Score indefinitely and their threat score is always increasing. You can manually decrease the threat score associated with an actor as described in Manually Adjusting the Threat Score—Optional. You can also add default time-out period to the Actor Changes active list by editing the TTL Days value in the active list editor. For example, you could set the TTL for the Actor Changes active list to 30 days and if no suspicious activity is detected for that actor, the actor is removed from the active list. Once the threat score of an actor reaches 500, the Actor Changes rule stops increasing the threat score for the actor. Such actors are phased off the list based on the TTL.

Customizing the Threat Score Associated with a Suspicious Activity—Optional

You can customize the threat scores associated with suspicious activities to reflect your environment. For example, if clearing an audit log is considered very suspicious in your environment, you might want to change the threat score associated with that activity in the Increase Actor Threat Score active list. For a full listing of the default suspicious activity rules and their associated threat score see Threat Score Associated with Suspicious Rules and Stored in the Active List .

To customize a threat score of an actor in the Actor Changes active list:

1. In the Navigator panel, select the Resources tab and the Lists option.
2. Expand the ArcSight Solutions/UBM/Actor Threat Score group.
3. Right-click the Actor Changes active list and select Show Entries.
4. Right-click an entry in the Viewer and select Edit.
5. Adjust the threat score appropriately.

The threat scores stored in the Increase Actor Threat Score active list (Threat Score Associated with Suspicious Rules and Stored in the Active List) correspond to the agent severity of correlation events generated by the suspicious activity rules as specified in Association Between Agent Severity and Threat Score Increase.

If you customize the threat score of any of the suspicious activity rules, you should also change the corresponding agent severity of the generated correlation event. For example, if you change the threat score associated with the Account Lockout rule from 1 to 5, ArcSight recommends that you also change the agent severity in the Actions tab of the Account Lockout rule from Medium to High.

Adding Your Suspicious Activity Rules—Optional

If you have custom rules that report suspicious activity in your environment, these rules can also increase the threat score associated with actors. The rule must be able to attribute events to actors. For more information, see Creating Custom Suspicious Activity Rules.

To add a rule to the Increase Actor Threat Score active list:

1. In the Navigator panel, select the Resources tab and the **Lists** option.
2. Expand the ArcSight Solutions/UBM/Actor Threat Score group.
3. Right-click the Actor Changes active list and select **Show Entries**.
4. To add an entry to the list, click the Add icon in the list header.
5. In the Entry editor of the Inspect/Edit panel, enter values for the required fields of the list:

- **Generator**—Enter the exact name of your suspicious activity rule. The case of the name must also match.
- **Threat Score**—Enter the appropriate threat score: 1, 5, or 25. The threat score associated with the rule should correspond to the agent severity of the correlation event generated by the rule as described in Association Between Agent Severity and Threat Score Increase.

6. Click**Add**.

Verify Configuration

After configuring this use case and the Suspicious Activity Use Case, verify that the actor threat score information is being populated.

1. In the Navigator panel, go to **Dashboards**.
2. Navigate to ArcSight Solutions/UBM/Actor Threat Score/.
3. Right-click Actor Threat Score Overview and select **Show Dashboard.**

Resources

The following table lists all the resources explicitly assigned to this use case and any dependent resources. Each resource can be accessed from the Actor Threat Score use case landing page: /All Use Cases/ArcSight Solutions/UBM/Actor Management, or their URI, for example: /All <Resource Type>/ArcSight Solutions/UBM/<Use Case>/<Resource Name>.

Resource	Description	Type
Monitor Resources		
Suspicious Level Actor Activity	This active channel shows activity attributable to actors on the actor threat score list whose threat score is in the suspicious range.	Active Channel
Watch Level Actor Activity	This active channel shows activity attributable to actors on the Actor Threat Score list whose threat score is in the watch range.	Active Channel
Malicious Level Actor Activity	This active channel shows activity attributable to actors on the Actor Threat Score list whose threat score is in the malicious range.	Active Channel
Actor Threat Score Changes	This active channel shows increases and additions to the Actor Threat Score active list.	Active Channel
Threat Score Overview	Displays information about the threat score for each affected user. It also serves as a means to delve deeper into the actual events. Before running this dashboard, make sure the following data monitor is enabled: /All Data Monitors/ArcSight Solutions/UBM/Overview/Threat Score Overview.	Dashboard

Resource	Description	Type
Malicious Level Actor Activity	This dashboard shows activity attributable to actors on the Actor Threat Score list whose threat score is in the malicious range.	Dashboard
Actor Threat Score Overview	This dashboard shows a summary of top threat score actors and the rules that have caused their threat scores to increase.	Dashboard
Top Threat Score Contributors	This dashboard shows information about top threat score contributor rules by threat score contribution, number of actors for which the rule triggered and the number of times the rule triggered.	Dashboard
Watch Level Actor Activity	This dashboard shows activity attributable to actors on the Actor Threat Score list whose threat score is in the watch range.	Dashboard
Suspicious Level Actor Activity	This dashboard shows activity attributable to actors on the Actor Threat Score list whose threat score is in the suspicious range.	Dashboard
Top Threat Score Contributors by Number of Actors	This query viewer shows the top rules that contribute to actor threat scores by number of unique actors for each rule.	Query Viewer
Threat Score Rule Firings for Actors on the Threat Score List	This query viewer shows correlation events that contribute to the Actor Threat Score.	Query Viewer
Actor Threat Score by Department	This query viewer shows the composite threat score for each department associated with actors on the Actor Threat Score active list.	Query Viewer
New Actors on Threat Score List	This query viewer shows the actors recently added to the Actor Threat Score active list.	Query Viewer
Top Threat Score Contributors by Number of Rule Firings	This query viewer shows the top rules that contribute to actor threat scores by the total number of times each rule was triggered.	Query Viewer
Top Actors on Threat Score List	This query viewer displays a chart of the actors with the highest threat scores.	Query Viewer
Top Threat Score Contributors by Threat Score Contribution	This query viewer shows the top rules that contribute to actor threat scores by the threat score contribution, which is the product of the total number of times the rule triggered and the threat score assigned to each rule.	Query Viewer
Threat Score with Actor Details	This query viewer shows the threat score for each actor along with actor base attributes.	Query Viewer
Recent Activity by Actors on the Threat Score List	This query viewer shows information from events attributed to actors on the Actor Threat Score active list over the last three hours.	Query Viewer
Top Actors on Threat Score List	This report displays a chart and table of the actors with the highest Threat scores.	Report
Top Threat Score Contributors	This report shows information that identifies the top rules that contribute to actor threat scores.	Report
Actor Threat Score Changes Over Time	This report shows all those events that identify all the changes to the specified actor's threat score over time.	Report

Resource	Description	Type
Actor Threat Score by Country or Region	This report shows a composite threat score for each country associated with actors on the Actor Threat Score active list.	Report
Department Threat Score Over Time	This report shows the composite threat score for a given department over time.	Report
Actor Threat Score by Title	This report shows a composite threat score for each title associated with actors on the Actor Threat Score active list.	Report
Actor Threat Score by Department	This report shows a composite threat score for each department associated with actors on the Actor Threat Score active list.	Report
Activity by Actors on Threat Score List	This report shows information from events attributed to actors on the Actor Threat Score active list.	Report
Login Attempts by Actors on Threat Score List	This report shows events that indicate login attempts to target systems and that are attributable to actors on the Actor Threat Score active list.	Report
New Actors on Threat Score List	This report shows actors newly added to the Actor Threat Score active list.	Report
Rule Firings for Actors on Threat Score List	This report displays correlation events that contribute to the Actor Threat Score.	Report
Library - Correlation Resources		
Actor Threat Score Reached Malicious Level	This rule is triggered when an actor's threat score reaches the malicious level. A notification is sent to the appropriate party for response.	Rule
Increase Actor Threat Score	This rule adds the attributable actor to the Actor Threat Score active list and calculates a new threat score for the actor.	Rule
Actor Threat Score Reduced	This rule triggers on audit events generated by ArcSight ESM when an actor's threat score is reduced in the Actor Threat Score active list.	Rule
Add Actor to Actor Threat Score List	This rule adds the attributable actor to the Actor Threat Score active list when a suspicious activity rule is triggered.	Rule
Actor Removed from Actor Threat Score List	This rule triggers on audit events generated by ArcSight ESM when an actor's entry is removed from the Actor Threat Score active list.	Rule
Library Resources		
Increase Actor Threat Score	This active list contains a list of suspicious activity rules and their customizable threat scores. When an actor causes one of these rules to trigger, their threat score is increased by the rule's threat score as defined in this list.	Active List
Account Authenticators	This active list is used by the actor global variables to determine what the Identity Management authenticator is, base on the event, so that an actor can be determined from event information.	Active List
Actor Threat Score	This list maintains a running threat score for actors exhibiting suspicious activity.	Active List
Last Events by Watch Level Actors	This data monitor shows the last events attributable to actors on the Actor Threat Score list whose threat score is in the watch range.	Data Monitor

Resource	Description	Type
Threat Score Moving Averages	This data monitor shows the moving average of the top Actor Threat Scores, sorted by percentage change.	Data Monitor
Top Malicious Level Actors	This data monitor shows the top active actors on the Actor Threat Score list whose threat score is in the malicious range.	Data Monitor
Malicious Level Actor Activity	This data monitor shows activity attributable to actors on the Actor Threat Score list whose threat score is in the malicious range.	Data Monitor
Watch Level Actor Activity	This data monitor shows activity attributable to actors on the Actor Threat Score list whose threat score is in the watch range.	Data Monitor
Threat Score Increases	This data monitors shows information from events indicating that an actor's Threat Score increased.	Data Monitor
Last Events by Malicious Level Actors	This data monitor shows the last events attributable to actors on the Actor Threat Score list whose threat score is in the malicious range.	Data Monitor
Last Events by Suspicious Level Actors	This data monitor shows the last events attributable to actors on the Actor Threat Score List whose threat score is in the suspicious range.	Data Monitor
Top Suspicious Level Actors	This data monitor shows the top active actors on the Actor Threat Score list whose threat score is in the suspicious range.	Data Monitor
Top Watch Level Actors	This data monitor shows the top active actors on the Actor Threat Score list whose threat score is in the watch range.	Data Monitor
Suspicious Level Actor Activity	This data monitor shows activity attributable to actors on the Actor Threat Score list whose threat score is in the suspicious range.	Data Monitor
AttributableActor	This global variable returns all the information for an actor, where the event to actor attribution is done using either attacker or target user name fields, or the source IP address. Note: To turn lookups based on the source IP address, in the Parameters tab, do not use the actorByAccountOrSourceIP local variable to lookup the actor, use the UUID field of the ActorByAccountID global variable instead.	Global Variable
ActorByAccountID	This global variable maps the account information in an event with an actor. The account information consists of the device vendor and product, and information derived from the attacker or target user name, with preference to the target user name.	Global Variable
ActorFromIPMap	This global variable returns an actor's UUID, full name, username used, and login type if the actor is associated with a source IP address.	Global Variable
ActorScoreFromActorThreatScoreUpdates	This global variable gets the threat score associated with an update to the Actor Threat Score active list.	Global Variable
ActorByUUIDThreatScore	This global variable retrieves an actor's threat score based on the UUID provided by the ActorByUUID global variable.	Global Variable

Resource	Description	Type
solnPatternDiscoveryConst	This variable returns a constant string that can be used in Pattern Discovery profiles when it is not required to specify either a Source or a Target event field.	Global Variable
ActorFromActorThreatScoreUpdates	This global variable gets details of the actor associated with updates to the Actor Threat Score active list.	Global Variable
solnGetAuthenticator	This global variable extracts the authenticator from the event by looking up the Account Authenticators list using event fields.	Global Variable
ActorByIPThreatScore	This global variable retrieves an actor's threat score based on the UUID provided by the ActorFromIPMap global variable.	Global Variable
solnGetUsername	This global variable returns user name in an event from target user name or attacker user name, with preference to the target user name.	Global Variable
AttributableActorThreatScore	This global variable retrieves an actor's threat score based on the UUID provided by the AttributableActor global variable.	Global Variable
ActorByAccountIDThreatScore	This global variable retrieves an actor's threat score based on the UUID provided by the ActorByAccountID global variable.	Global Variable
ActorByUUID	This Actor global variable looks for a UUID in Device Custom String1, and retrieves the Actor with that UUID.	Global Variable
Events with ActorByAccountID	This field set selects the fields appropriate for viewing events correlated with actor and can be customized for the UBM active channels.	Field Set
Threat Score Increases	This field set can be used for viewing increases and additions to the Actor Threat Score active list.	Field Set
Events with AttributableActor	This field set selects the fields appropriate for viewing events correlated with either account-id or IP address and can be customized for the UBM active channels.	Field Set
Events with ActorByUUID	This field set selects the fields appropriate for viewing events correlated with actor and can be customized for the UBM active channels.	Field Set
Deleted Entry from Actor Threat Score List	This filter identifies events that indicate an entry has been deleted from the Actor Threat Score active list.	Filter
Activity by Actors on Threat Score list	This filter selects events attributable to actors on the Actor Threat Score list.	Filter
Address or Username Present	This filter checks whether any of attacker address, attacker username, or target username are present in the event.	Filter
Target Username is a System Account	This filter selects events in which the target user name is a system account.	Filter
Changes to the Actor Threat Score List	This filter captures all events that identify changes to the Actor Threat Score List.	Filter
Malicious Level Actor Activity	This filter selects activity attributable to actors on the Actor Threat Score list whose threat score is in the malicious range.	Filter

Resource	Description	Type
Target User Name is NOT NULL	This filter selects events in which the attacker user name field is populated.	Filter
Login Attempts	This filter selects any attempts at logging into systems. It excludes machine logins into Microsoft Windows systems.	Filter
Threat Score Increases	This filter selects events indicating that an actor's Threat Score increased.	Filter
Attacker User Name is a System Account	This filter selects events in which the attacker user name is a system account.	Filter
Windows Events with a Non-Machine User	This filters identified Microsoft Windows events that have a non machine/system user either in the attacker or the target fields.	Filter
Active List Entry Updated	This filter identifies events which indicate that an active list entry has been updated.	Filter
Watch Level Actor Activity	This filter selects activity attributable to actors on the Actor Threat Score list whose threat score is in the watch range.	Filter
Threat Score Contributors	This filter selects rule trigger events that contribute to the Actor Threat Score.	Filter
ActorByAccountID is NULL	This filter selects events which can not be correlated to an actor based on the attacker or target user name fields.	Filter
Username Present	This filter checks whether any of attacker username, or target username are present in the event.	Filter
Suspicious Level Actor Activity	This filter selects activity attributable to actors on the Actor Threat Score list whose threat score is in the suspicious range.	Filter
Actor Threat Score Updated	This filter selects events that can be associated with an update to the Actor Threat Score active list.	Filter
ActorByAccountID is NOT NULL	This filter selects events which can be correlated to an actor based on the attacker or target user name fields.	Filter
Target User Name is NULL	This filter selects events in which the target user name field is not populated.	Filter
Windows Events	This filter selects all events in which the device product field is Microsoft Windows.	Filter
Actor Threat Score NULL	This filter selects events for which the attributable actor does not have an established threat score.	Filter
Rule Firings for Threat Score Contributors	This profile detects patterns of actor threat score correlation events.	Profile
Threat Score Contributors - Trend	This query gets aggregated information about correlation events for rules that contribute to an actor's threat score.	Query
Top Threat Score Contributors	This query identifies the top rules that contribute to actor threat scores.	Query
Activity by Actors on Threat Score List	This query selects information from events attributed to actors on the Actor Threat Score active list.	Query

Resource	Description	Type
Top Threat Score Contributors by Number of Actors	This query identifies the top rules that contribute to actor threat scores by number of unique actors for each rule.	Query
Actor Threat Score by Title	This query returns a composite threat score for each title associated with actors on the Actor Threat Score active list.	Query
Actor Threat Score Changes Over Time	This query selects all those events that identify all the changes to the specified actor's threat score over time.	Query
Threat Score with Actor Details	This query retrieves threat score for each actor along with actor base attributes.	Query
Threat Score Rule Firings for Actors on the Threat Score List	This query selects correlation events that contribute to the Actor Threat Score.	Query
Actor Threat Score by Country or Region	This query returns a composite threat score for each country associated with actors on the Actor Threat Score active list.	Query
Top Threat Score Contributors by Threat Score Contribution	This query identifies the top rules that contribute to actor threat scores by the threat score contribution, which is the product of the number of times each rule triggered and the threat score assigned to each rule.	Query
All Actions for Actor	This query gets aggregated information about events that might be attributable to actors.	Query
Department Threat Score Over Time	This query gets the composite threat score for a given department over time.	Query
New Actors on Actor Threat Score List	This query selects the actors recently added to the Actor Threat Score active list.	Query
Login Attempts by Actors on Threat Score List	This query selects login attempts attributable to actors on the Actor Threat Score active list.	Query
Top Threat Score Contributors by Number of Rule Firings	This query identifies the top rules that contribute to actor threat scores, by the total number of times each rule triggered.	Query
Actor Threat Score by Department	This query returns a composite threat score for each department associated with actors on the Actor Threat Score active list.	Query
Top Actors on Threat Score List	This query selects the actors with the highest threat scores.	Query
IP Address to Actor Map	This session list tracks the IP addresses that can be associated with actors. Typically, these IP addresses will belong to single-user machines.	Session List
Weekly Department Threat Score	This trend collects a composite threat score for each department that has actors on the threat score list and records that score weekly.	Trend
All Actions for Actor	This hourly trend collects aggregated information about events that might be attributable to actors.	Trend
Threat Score Contributors	This trend captures a summary of all rules that trigger and contribute to the threat scores of actors.	Trend

Suspicious Activity Use Case

The Suspicious Activity use case provides resources that can be used to discover and analyze suspicious activity occurring on your network. When triggered, the suspicious activity rules can contribute to the resources of the Actor Threat Score Use Case.

This use case provides the following:

- Reports, query viewers and dashboards that provide information about suspicious activity and suspicious activity rule firings for actors, departments and job titles
- Pattern Discovery profiles that detect patterns of suspicious activity and rule firings across actors

This use case reports on the following suspicious activity:

- Account Management
- At Risk User Activity
- Traffic from an Area of Concern
- Database Access Attempts
- Email Failures
- General Security Breaches
- Information Leakage
- Network Based Anomaly Detection
- Physical Location Anomalies
- Policy Violations
- Printing
- Role Violations
- Web Interaction

The Suspicious Activity Use Case rules determine the actor attributable to an event, using global variables.

Here are some examples:

- The Account Lockout Rule rule invokes the ActorByTargetName global variable because the triggering account lockout event populates the target user name field with the user name associated with the attributable actor.
- The Audit Log Cleared rule invokes the ActorByAccountID global variable because the triggering audit log cleared event might populate either the attacker or target user name field with the user name associated with the attributable actor.

- The Anonymous Proxy Access might not have the user name, so the AttributableActor global variable attempts to determine the attributable actor using source IP of the login if the account ID is not available.

Each suspicious activity rule takes the actor's UUID and full name returned from the global variable and populates the following event fields in the generated correlation event:

deviceCustomString1 field with the UUID

deviceCustomString2 field with full name of the actor

Regardless of which global variable the rule invokes to get the attributable actor, the UUID and full name is placed into the deviceCustomString1 and deviceCustomString2 fields of correlation event for consumption by the resources in the Actor Threat Score Use Case. For more information, see Actor Threat Score Use Case.

The UUID is the Universally Unique Identifier for the actor assigned by the Identity Management System.

Account Management

The Suspicious Activity Use Case reports on the following potential misuse of accounts:

- Windows account lockouts—user accounts that have been disabled after too many failed login attempts have occurred
- Account activity from an account that has been disabled
- Account activity from unaccountable user ID—a user ID that not be correlated to an identity
- Use of default vendor accounts
- Creation of a local administrator account on Windows systems

At Risk User Activity

The Suspicious Activity Use Case reports on the following suspicious activity by at-risk identities represented by actors. An at-risk actor represents a user that should be monitored at a higher level of scrutiny, such as:

- Contractors
- Known disgruntled employees
- New hires
- Employees that have given notice
- Actors exhibiting suspicious behavior and therefore listed in the Actor Changes active list

The set of identities that are considered at risk is defined by the filter.

The following suspicious behavior is tracked for at-risk actors:

- After hours building access
- After hours database access
- Information leakage of company information
- Information leakage of personal information
- Printing of resumes
- Emailing resumes

Traffic from an Area of Concern

The Suspicious Activity Use Case monitors network traffic to countries and web sites that might be of a concern to your organization.

Database Access Attempts

The Suspicious Activity Use Case reports on the following suspicious database access attempts:

- A successful brute force login
- Multiple failed logins by the same user targeting a database

Email Failures

The Suspicious Activity Use Case reports on rejected emails and email errors.

General Security Breaches

The Suspicious Activity Use Case reports on breaches of general security practices and policies, such as:

- Clearing of host audit logs
- Password resets without a preceding account lockout
- Same user using different user names

Information Leakage

The Suspicious Activity Use Case monitors for information leakage, such as:

- Suspicious printing activities
- Communications with competition

- Information leakage is when sensitive data is intentionally or accidentally leaked from an organization to an outside target. Sensitive information is whatever your organization considers valuable or confidential, such as personal records, banking information or national secrets.

Network Based Anomaly Detection

The Suspicious Activity Use Case monitors the following network-based activities:

- New hosts added to the network
- Anomalous network traffic
- New services added to machines on the network
- Scans

Physical Location Anomalies

The Suspicious Activity Use Case monitors for physical location anomalies by tracking the badge status of employees and correlating it other factors:

- Reporting internal system use by an identity not physically present in the building.
- Reporting potential compromised VPN accounts—VPN authentications from identities who are physically present in the building.

Policy Violations

The Suspicious Activity Use Case monitors when policy violations occur, such as:

- Windows security software is disabled
- An attempt has been made to browse the Windows IPC system share

Printing

The Suspicious Activity Use Case monitors suspicious printing activities, such as:

- Printing after hours
- Printing suspicious documents

Role Violations

The Suspicious Activity Use Case monitors and reports on role violations involving an identity. A role violation occurs when an identity access systems that belong to a different department or they do not have proper role to access. In addition, authorizations on monitored systems such as privilege grants or assignments to groups can be analyzed for consistency with role information stored in the Identity Management System. For example, if Jane Doe was granted the DBA role on a database system but in the Identity Management System she was not granted this role, this role violation would be reported.

The resources provided in the Suspicious Activity Use Case enables auditors, analysts, and managers to provide the following services:

- Monitor, report, and alert on user access to monitored systems for which they do not have the proper role
- Monitor, report, and alert on user access to monitored systems belonging to a different department
- Detect when roles and privileges assigned on monitored systems do not align with assignments in Identity Management System
- Generate role violation reports for a specific identity, employee type, role, or department

Web Interaction

The Suspicious Activity Use Case monitors the following identity interactions with the web:

- Use of known public proxy servers—This activity could indicate that someone is trying to hide their web surfing activities.
- Interactions with known hacker Web sites—This activity could indicate that someone is trying to engage in malicious activity by downloading hacker tools or accessing hacker-related information.
- Interactions with known public job Web sites— This activity could indicate that someone is trying to either post his resume online or is looking for new job opportunities.

Devices

The following devices can supply events to this use case:

- Intrusion Detection System
- Intrusion Prevention System
- Network Based Anomaly Detection
- Database
- Operating System

- Firewall
- Virtual Private Network
- Vulnerability Assessment
- Identity Management System
- Policy Management
- Network Equipment
- Content Security, Web Filtering
- Physical Security Systems
- Antivirus
- Wireless
- Application

All the devices listed above can supply events to this use case but the resources will only process events from devices, when the device generates events that can be attributed to specific actors.

Categorize Assets

This use case requires categorization of monitored assets into the UBM network domains. For more information, see . For example, a role violation is detected if a user in the Human Resources department accesses a server asset categorized as Finance.

This use case contains resources with conditions that check if incoming events involve assets categorized with the asset categories listed in following table. Classify assets appropriately with these categories to trigger the resources during run time.

Asset Categories used by Suspicious Activity Use Case

Asset Category	Configuration
Competition	Categorize the assets of the competition. You can categorize the competition assets and/or add the competition domains to the Competition Domains active list. For more information, see Active Lists.
Destinations/Anonymous Proxies	Categorize additional public proxy servers. Events sent via a proxy server could indicate that someone is trying to hide their identity. By default, the following proxy servers are categorized: • anonybrowser.com • anonymizer.com • proxify.com • proxify.com1 • proxify.com2 • proxify.com3 • proxify.com4 • pureprivacy.com • webproxy.kaxy.com

Asset Category	Configuration
Destinations/Career Sites	Categorize additional job hunting web sites. By default, the following career web sites are categorized: • FindAJob.org • Get-A-Job-Now.com • careerbuilder.com • careerpage.org • dice.com • hotjobs.com • iHireJobNetwork.com • ieee.careercast.com • indeed.com • jobdeputy.com • linkedin.com • monster.com • monster.com1 • officialjobboard.com • thingamajob.com • web.hj.scd.yahoo.com
Destinations/Hacker Sites	Categorize additional hacker tool web sites. By default, the following hacker tool web sites are categorized: • 2600.com • astalavista.com • hackerhighschool.org • insecure.org • metasploit.com • nessus.org • packetstormsecurity.org
Destinations/Prohibited Sites-Other	This category is not explicitly used by UBM solution resources, but can be used to categorize other types of prohibited destinations.

The Classification Level - Lower to Higher and Classification Level - Higher to Lower filters uses the security level categories, Confidential, Secret, Top Secret. Classify your assets into the appropriate Information Classification/National Security category.

Configure Resources

Configure the following types of resources for this use case:

Active Lists

Configure the active lists listed in the following table for this use case. These active lists are available from the following location:

```
ArcSight Solutions/UBM/Suspicious Activity
```

Populate Suspicious Activity Active Lists

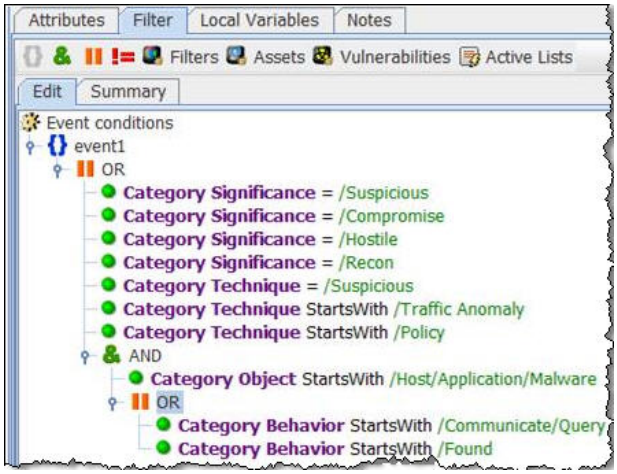
Active List	Description	Configuration
Competition Domains	This active list is used to define DNS domain names of competitive companies.	Populate with competition DNS domain names.
Countries of Concern	This active list contains the country code of countries with whom information exchange might be suspect.	Add ISO country codes for countries of concern from http://www.iso.org/iso/en/prods-services/iso3166ma/02iso-3166-code-lists/list-en1.html
Default Vendor Accounts	This active list contains default user accounts that ship with products.	Optional—By default, this list is populated with default vendor user accounts provided with common applications and operating systems. Add any additional vendor user accounts for applications and operating systems used by your organization.
Disgruntled Actors	This list contains the full names and UUID of disgruntled identities. The activity of the actors on this list are monitored at a higher level of scrutiny	Add the UUID and full name of any disgruntled employees. For more information, see . This list should be maintained manually.
New Hire Actors	This active list contains the full names and UUID of newly hired employees. The activity of the actors on this list are monitored with greater suspicion.	Optional—This lists is automatically populated when new actors are added to the IDM. You might want you set the time period that a new hire is considered new, by editing the TTL Days value for this active list in the active list editor.

Active List	Description	Configuration
Notice-Given Actors	This active list contains the full names and UUID of employees who have given notice. The activity of the actors on this list can be monitored with a higher level of scrutiny.	Add UUID and the full name of employees who have given notice. For more information, see . This list should be maintained manually.
Public Webmail	This list contains all the DNS domains for public webmail servers, for example gmail.com. This list is used to detect when large emails are sent to those domains, indicating suspicious activity.	Optional—By default, this list is populated with the set of default public Webmail servers. Add additional public Webmail servers.
Role Violations	The rule places an actor on the Actor Changes active list when an actor accesses a target system belonging to a department to which they do not belong, and for which they do not have the defined role. The rule triggers the first time an actor/target system combination is detected. Subsequent role violations by the same actor/target system combination are not reported unless a time out period is specified.	Optional—This is automatically populated with actors by Actor Changes rule. To configure the Actor Changes rule to report subsequent role violations after a specified time period, edit the list and set the one of the TTL fields to a value.

Filters

Configure the following filters for this use case:

- **Suspicious Activity/General Security/Suspicious Activity filter**— This filter uses event categorization to determine which events are suspicious and drives the Suspicious Activity use case. To specify additional event types as being suspicious, add additional conditions to this filter.



- **Suspicious Activity/Role Violations/Role Violations** filter—This filter selects events in which an identity accesses a target system belonging to a department to which they do not belong, and for which they do not have the defined role. For example, a role violation is detected if a user in the Human Resources department accesses a

server asset categorized as Finance. This is only intended as a template. Configure this filter to match your organization user roles. Add additional conditions as needed.

Rules

By default, all the rules in this use case are disabled. Enable only the rules that are significant for your organization. Each suspicious activity rule contains an action that generates a correlation event and by default these rule actions are enabled.

Enabling many rules can impact the performance of the ESM Manager. Significant tuning might be required for the UBM solution rules.

Trends and Queries

Reports and query viewers in this use case are based on the trends listed below.

Before enabling the trends listed below, verify that these trends collect the expected events for your environment. In addition, you might want to customize the trend before enabling. For more information, see .

Enable the following trends for this use case:

- Threat Score Contributors—This trend is included with the Actor Threat Score Use Case. Several resources in this use case require that this trend be enabled.
- All Actions for Actor—This trend is included with the User Activity Monitoring Use Case. Several resources in this use case require that this trend be enabled.

Creating Custom Suspicious Activity Rules

If you have custom rules that report suspicious activity in your environment, these rules can also increase the threat score associated with actors. The rule must be able to attribute events to actors.

You can create custom suspicious activity rules that report suspicious activity in your environment. The rule must be able to attribute events to actors. In your rule, use one of the global variables (listed in) to attribute the actor to the suspicious activity.

To create your own rule, you can copy one of the following template rules and customize it for your suspicious activity.

- Suspicious Activity Template - ActorByAccountID
- Suspicious Activity Template - AttributableActor

Add the rule to the Increase Actor Threat Score active list with the appropriate threat score. For detailed instructions, see Adding Your Suspicious Activity Rules—Optional.

Verify Configuration

After configuring this use case, verify events are being processed by the suspicious activity rules by viewing the Actor Changes active channel:

1. In the Navigator panel, go to **Active Channels**.
2. Navigate to ArcSight Solutions/UBM/Suspicious Activity.
3. Right-click Actor Changes and select **Show Active Channel**.

All rule fire events for this use case should display.

Resources

The following table lists all the resources explicitly assigned to this use case and any dependent resources. Each resource can be accessed from the Suspicious Activity use case landing page: /All Use Cases/ArcSight Solutions/UBM/Actor Management, or their URI, for example: /All <Resource Type>/ArcSight Solutions/UBM/<Use Case>/<Resource Name>.

Resource	Description	Type
Monitor Resources		
Suspicious Activity	This active channel shows all suspicious events.	Active Channel
Role Violations	This active channel displays events in which an actor accesses a target system for which they do not have the defined role.	Active Channel
Activity from Disabled Actors	This active channel shows events in which the actor associated with the attacker or target user name has been disabled.	Active Channel
Suspicious Activity Rule Firings	This active channel shows correlation events from the Suspicious Activity use case.	Active Channel
Information Leak Events	This active channel shows information leak events.	Active Channel
Hacker Tool Web Site Access	This active channel shows all activity where the target is a known hacker tool Web site.	Active Channel
Job Hunting Web Site Access	This active channel shows all activity where the target is a known job hunting Web site.	Active Channel
Top Suspicious Actors Overview	Displays a summary of top threat score actors.	Dashboard

Resource	Description	Type
Network Based Anomaly Detection	This dashboard shows network-based anomaly detection traffic.	Dashboard
Suspicious Activity Rule Firings	This dashboard shows a composite view of suspicious activity correlation events across actors, departments and job titles.	Dashboard
Information Leak by Data Type	This dashboard shows events indicating possible information leaks.	Dashboard
Suspicious Activity	This dashboard shows a composite view of suspicious activity across actors, departments and job titles.	Dashboard
Leaked Files	This filter shows all leaked files.	Dashboard
Information Leak Status	This dashboard shows traffic related to information leaks.	Dashboard
Role Violations	This dashboard shows event graphs of role violations by employee type and department.	Dashboard
Classification Level Violations	This dashboard shows traffic that violates information classification rules	Dashboard
Email Errors	This dashboard shows email related errors.	Dashboard
Competitive Email Communications	This dashboard shows events indicating emails to or from a competitor's email DNS domain.	Dashboard
Concerns	This dashboard shows events that are a concern for many organizations. Examples include traffic to or from countries of concern, possible data leaks, and national security concerns.	Dashboard
Top Actors with Suspicious Activity Rule Firings	This query viewer shows the top actors by number of UBM suspicious activity correlation events.	Query Viewer
Suspicious Activity Rule Firings	This query viewer shows correlation events for UBM suspicious activity rules.	Query Viewer
Top Job Titles with Suspicious Activity Rule Firings	This query viewer shows the top job titles by number of UBM suspicious activity correlation events.	Query Viewer
Top Suspicious Activity Rules	This query viewer shows the top suspicious activity rules by the total number of times each rule triggered.	Query Viewer
Top Departments with Suspicious Activity Rule Firings	This query viewer shows the top departments by number of UBM suspicious activity correlation events.	Query Viewer
Traffic to Competition	This report details all communication with competitive organizations as defined by the asset categories or the Competition active list.	Report
Suspicious Document Transferred	This report shows events indicating that a suspicious document has been transferred.	Report
Suspicious Activity Rule Firings for Actor	This report shows information about UBM suspicious activity correlation events for the specified actor.	Report
Suspicious Activity by Privileged Actors	This report shows information from events indicating suspicious activity by privileged actors.	Report

Resource	Description	Type
Failed Building Access Events	This report shows events indicating failed building access.	Report
Role Violations for Department	This report shows a summary chart and detailed table of role violations for the specified department.	Report
Specific Document Printed	This report shows events indicating that the specified document has been printed.	Report
Role Violations by Target Asset Role	This report shows a summary chart and detailed table of role violations by target asset role.	Report
Oracle Privilege Grants	This report shows privileges granted in Oracle.	Report
Role Violations for Target Asset Role	This report shows a summary chart and detailed table of role violations for the specified target asset role.	Report
Information Leak - Top Rule Firings	This report shows the top information leak rules triggered.	Report
DBA_USERS Access	This report shows all SELECT operations on the dba_users table in Oracle.	Report
Oracle NOAUDIT	This report shows all the users who have had auditing disabled.	Report
Suspicious Notice-Given User Activity	This report shows suspicious events by actors in the Notice Given list.	Report
Suspicious Disgruntled User Activity	This report shows suspicious events by actors on the Disgruntled list.	Report
Role Violations by Employee Type	This report shows a summary chart and detailed table of role violations by employee type.	Report
Oracle Users Created	This report shows all the new users that have been created within Oracle.	Report
Files Emailed	This report shows all files that have been emailed.	Report
DBA_USERS UPDATES	This report shows all updates to the dba_users table in Oracle.	Report
Suspicious Activity Rule Firings for Department	This report shows information about UBM suspicious activity correlation events for the specified department.	Report
All Suspicious Activity for Department	This report shows the actor full name, vendor, product, event name, and count of all suspicious events that can be correlated to an actor belonging to the specified department.	Report
Oracle Grant Role DBA	This report shows all successful dba role grants by the user who executed the grant.	Report
Failed Database Authentication Review	This report shows all failed authentications to databases.	Report
Resumes Emailed	This report shows events indicating that a resume was emailed.	Report
Confidential Document To Competition	This report shows all users who have sent a confidential document to a competitor.	Report
Audit Table Delete	This report shows all deletions from the audit table.	Report

Resource	Description	Type
Specific Document Transferred	This report shows events indicating that the specified document was transferred.	Report
Suspicious Activity by Threat Score Actors	This report shows information from suspicious events attributed to actors having a threat score greater than zero.	Report
Traffic to Countries of Concern	This report details all communication with countries of concern as defined by the Countries of Concern active list.	Report
Database Table Access Review	This report shows all database tables that have been accessed, and the users accessing them.	Report
Printing Suspicious Documents	This report shows events indicating the printing of suspicious documents.	Report
Role Violations for Employee Type	This report shows a summary chart and detailed table of role violations for the specified employee type.	Report
Suspicious Activity Rule Firings for Job Title	This report shows information about UBM suspicious activity correlation events for the specified job title.	Report
Privileges Granted without Proper Role	This report shows events indicating that elevated privileges were granted to a non-privileged actor.	Report
All Suspicious Activity for Role	This report shows the actor's full name, unique ID, product, event name, and count of all suspicious events that can be correlated to an actor having the specified role.	Report
Audit Options Table Delete	This report shows any user attempting to delete their audit settings directly from the table audit options table.	Report
Suspicious New Hire Activity	This report shows suspicious events from new hires.	Report
Database Authentication Review	This report shows all successful database authentications.	Report
All Suspicious Activity for Employee Type	This report shows the actor full name, vendor, product, event name, and count of all suspicious events that can be correlated to an actor having the specified employee type.	Report
Suspicious Activity Rule Firings for Role	This report shows information about UBM suspicious activity correlation events for the specified role.	Report
Activity from Disabled Actors	This report shows information from events in which the actor associated with the attacker or target user name in the event has been disabled.	Report
After Hours Database Accesses	This report shows events indicating after hours database access.	Report
Suspicious Activity Rule Firings for Employee Type	This report shows information about UBM suspicious activity correlation events for the specified employee type.	Report
Role Violations by Department	This report shows a summary chart and detailed table of role violations by department.	Report
DBA_USERS DELETES	This report shows all delete operations to the dba_users table in Oracle.	Report
Rejected Email Senders	This report shows the sender, relay, and time of rejected email events.	Report

Resource	Description	Type
All Suspicious Activity	This report shows information from all suspicious events that can be correlated to an actor.	Report
Printing Activity After Hours	This report shows events indicating after hours printing activity.	Report
Library - Correlation Resources		
Data Manipulated T1565	Detects attempts to insert, delete, or manipulate data in order to influence external outcomes or hide activity, thus threatening the integrity of the data.	Rule
Successful Brute Force Account Login T1110	Detects each time a user logs in successfully after multiple unsuccessful attempts in a short time. This rule depends on an entry in the active list: Brute Force Attempts.	Rule
Unsuccessful Brute Force Login Attempts T1110	Detects multiple unsuccessful logins to the account in a short time. This rule adds an entry to the active list: Brute Force Attempts.	Rule
Possible LSASS Memory Dumping T1003.001	Detects when ProcDumps or MiniDumps via rundll32 are used to dump the memory space of Lsass.exe.	Rule
Possible Data Exfiltration T1041	Detects transfers of suspicious amounts of data to any host outside the network.	Rule
Possible Data Exfiltration to External Website via PowerShell T1041	Detects possible data exfiltration to external website via PowerShell.	Rule
Silver Ticket Attack Detected T1558.002	Detects silver ticket attacks. A silver ticket forges authentication tickets that the system creates when an attacker steals a user's password from Active Directory (AD). This ticket is used to forge ticket-granting service tickets, allowing unauthorized access to targeted resources.	Rule
Golden Ticket Attack Detected T1558.001	Detects golden ticket attacks. A golden ticket attack occurs when an attacker tries to access a domain through user data stored in the Microsoft Active Directory (AD). This allows attackers to bypass authentication, gaining access to the AD and its resources.	Rule
Attempted Bypass of MFA T1111	Detects attempts to bypass MFA. Adversaries may target multi-factor authentication (MFA) mechanisms to gain access to credentials that can be used to access systems, services, and network resources.	Rule
Multiple MITRE Techniques Against the Same Actor	Detects sets of three MITRE ATT&CK Techniques against the same actor.	Rule

Resource	Description	Type
Multiple MITRE Techniques Against the Same Department	Detects sets of three MITRE ATT&CK Techniques against specific department.	Rule
Possible Scrapping of Outlook Inbox via PowerShell T1114.001	Detects possible scrapping of outlook inbox via PowerShell.	Rule
Multiple Systems Logged into by Same User in a Short Time T1078.002	Detects each time a user logs in successfully into multiple systems in a short time.	Rule
Consecutive Unsuccessful Logins into Same Machine by Different Users T1078.002	Detects consecutive unsuccessful logins into same machine by different users in a short time.	Rule
Possible Automated Collection via PowerShell T1119	Detects possible automated collection of files by PowerShell.	Rule
Consecutive Unsuccessful Logins to Same Actor from different Countries T1110	Detects sets of three consecutive unsuccessful logins to the same actor from three different countries.	Rule
Information Leakage from Database T1213	Detects information leakage from a database.	Rule
Printing Suspicious Documents	This rule detects any document names being printed that match the filter for suspicious documents.	Rule
Account Lockout	This rule detects Microsoft Windows account lockout events and adds the target username and associated actor to the Account Lockouts active list.	Rule
Anonymous Proxy Access	This rule triggers on connections to anonymous proxy servers. This activity could indicate that someone is attempting to access prohibited sites or hide their web surfing activity.	Rule
Hacker Tool Website Access	This rule monitors network traffic targeting known hacker Web sites. The servers are assets categorized as Hacker Sites. This activity could indicate that someone is trying to engage in malicious activity by downloading hacker tools or accessing hacker-related information.	Rule
Activity from Disabled Actor	This rule triggers on events in which the actor associated with the attacker or target user name in the event has been disabled.	Rule
Role Violation	This rule triggers on events in which an actor accesses a target system belonging to a department to which they do not belong, and for which they do not have the defined role.	Rule

Resource	Description	Type
Job Hunting	This rule monitors network traffic targeting known public job Web sites. The job sites are assets categorized as Career Sites. This activity could indicate that someone is trying to either post his resume online or is looking for new job opportunities.	Rule
After Hours Building Access by At Risk Actor	This rule looks for after hours building access attempts by high risk actors.	Rule
Non-DBA Added to Oracle DBA Role	This rule triggers on events indicating that an Oracle user account was granted the role of dba, but the actor owning the account is not defined as a dba in the actor model.	Rule
Login to Known Shared Account by Actor	This rule triggers on login events to known shared accounts.	Rule
Failed Building Access	This rule detects failed building access.	Rule
Large Email to Public Webmail Servers	This rule looks for large email messages being sent to public Web mail accounts such as Yahoo.	Rule
Activity from Badged Out Employee	This rule detects network activity on an internal network segment even though the employee is not physically present in the building.	Rule
Database Brute Force Login Success	This rule looks for brute force database logins followed by a successful login.	Rule
Physical Plus VPN Access	This rule detects possible compromised VPN accounts by looking for VPN authentications from actors that are physically present in the building.	Rule
Suspicious Activity Template - ActorByAccountID	This rule can be used as a template to add custom suspicious activity rules to your UBM deployment. In this rule, the attributable actor is determined by the ActorByAccountID global variable. Add your condition first before enabling it.	Rule
Using Different Usernames	This rule detects people connecting with two different user names.	Rule
Leak of Company Information	This rule triggers when a leak of company information is detected.	Rule
Multiple Failed Database Access Attempts	This rule looks for multiple failed logins by the same user targeting a database.	Rule
After Hours Database Access by At Risk Actor	This rule detects database access after hours by at-risk actors.	Rule
Resume Emailed by At Risk Actor	This rule triggers if high risk actors send resumes through email.	Rule
Local Admin Created	This rule identifies the creation of a local administrator account in Microsoft Windows.	Rule
Network Scan	This rule triggers when network scan events are reported, indicating reconnaissance activity.	Rule
Traffic From Competition	This rule monitors for connections coming from machines classified as belonging to competitors.	Rule
Large Email to Competition	This rule detects emails sent to competitors.	Rule

Resource	Description	Type
Excessive Printing	This rule looks for excessive printing activity.	Rule
Traffic to Country of Concern	This rule monitors for traffic going to countries of concern. Countries of concern can be configured using the Countries of Concern active list.	Rule
Suspicious Activity Template - AttributableActor	This rule can be used as a template to add custom suspicious activity rules to your UBM deployment. In this rule, the attributable actor is determined by the AttributableActor global variable. Add your condition first before enabling it.	Rule
Compromise - Attempt	This rule detects any attempt to compromise a device from a source that is not listed on a trusted active list. It triggers whenever an event is categorized as attempt and compromise. On the first event, agent severity is set to high, the attacker address is added to the Hostile active list, and the target address is added to the Hit active list.	Rule
Suspicious Activity by Privileged Actor	This rule triggers on detection of suspicious activity caused by a privileged user.	Rule
VPN Login from Competition Domain	This rule triggers on events indicating a VPN login has occurred, and the source IP address belongs to a competitor's domain.	Rule
Leak of Personal Information	This rule triggers when a leak of personal information is detected.	Rule
IPC Share Browsing	This rule looks for any attempts to browse Microsoft Windows system shares.	Rule
Printing Confidential Documents	This rule detects any document names being printed that match the filter for confidential documents.	Rule
Traffic to Competition	This rule monitors for traffic going to competitors.	Rule
Audit Log Cleared	This rule monitors for the clearing of host audit logs.	Rule
Security Software Disabled	This rule is triggered when a Microsoft Windows security software service has been disabled.	Rule
Default Vendor Account Attempt	This rule triggers when a user tries to access a default vendor account. Default vendor account identifiers are maintained in the Default Vendor Accounts active list.	Rule
Printing After Hours	This rule detects printing activity after hours.	Rule
Library Resources		
Badged In Actors	This active list maintains a list of actors who have badged into the building. By default, actors expire from the list in 1 day.	Active List
Public Webmail	This list contains all the DNS domains for public webmail servers. For example hotmail.com. This list is used to detect when big emails are sent to those domains, being a possible information leak.	Active List
Countries of Concern	This active list contains the country code of countries with whom information exchange might be suspect.	Active List
Competition Domains	This active list is used to define DNS domain names of competitors, and can be used to detect information leakage to those domains.	Active List

Resource	Description	Type
Disgruntled Actors	This active list contains a list of disgruntled actors. It should be populated with actors who require additional monitoring.	Active List
Increase Actor Threat Score	This active list contains a list of suspicious activity rules and their customizable threat scores. When an actor causes one of these rules to trigger, their threat score is increased by the rule's threat score as defined in this list.	Active List
Notice-Given Actors	This active list contains a list of actors scheduled for termination, which might require a higher level of monitoring.	Active List
Default Vendor Accounts	This active list contains user accounts that might ship as standard accounts with many vendors products.	Active List
Privileged User Roles	This active list is used to define user groups with elevated privileges.	Active List
Account Authenticators	This active list is used by the actor global variables to determine what the Identity Management authenticator is, base on the event, so that an actor can be determined from event information.	Active List
Role Violations	This active list contains a list of actors who have accessed systems for which they do not have the correct role or department. Further role violation events will not occur as long as the Actor and Target Asset Group are in this list.	Active List
Known Shared Accounts	This active list maintains a list of known shared accounts per application. Note that all account IDs must be in uppercase and the Application field must be the same as what appears in the Device Product event field.	Active List
New Hire Actors	This active list maintains a list of new hire actors. The default expiration is two weeks from the date the actor is added to the system.	Active List
Actor Threat Score	This list maintains a running threat score for actors exhibiting suspicious activity.	Active List
Hacker Sites	This is a solutions asset category.	Asset Category
Secret	This is a site asset category.	Asset Category
Top Secret	This is a site asset category.	Asset Category
Protected	This is a site asset category.	Asset Category
Confidential	This is a solutions asset category.	Asset Category
National Security	This is a solutions asset category.	Asset Category
Anonymous Proxies	This is a solutions asset category.	Asset Category

Resource	Description	Type
Career Sites	This is a solutions asset category.	Asset Category
Network Domains	This is a solutions asset category.	Asset Category
Competition	This is a solutions asset category.	Asset Category
Suspicious Activity Rule Firings	This data monitor shows the last suspicious activity rules triggered and the actor responsible.	Data Monitor
Top Actors with Suspicious Activity	This data monitor shows the top actors exhibiting suspicious activity.	Data Monitor
Last Company Concerns	This data monitor shows the latest traffic flagged as a potential concern for the company.	Data Monitor
Top Information Leaks by Destination Address	This data monitor shows the top information leaks by destination address.	Data Monitor
New Hosts	This data monitor shows new hosts detected on the network.	Data Monitor
Top Failed Email Senders	This data monitor shows the senders causing the most errors with their email traffic.	Data Monitor
Top Departments with Suspicious Activity	This data monitor shows the top departments exhibiting suspicious activity.	Data Monitor
Role Violations by Department - Event Graph	This data monitor shows an event graph of role violations by department and actor along with the asset category of the target system.	Data Monitor
Top Information Leaks by User	This data monitor shows the top information leaks by user.	Data Monitor
Last 10 Information Leak Events	This data monitor shows the last ten events classified as information leaks.	Data Monitor
Top Company Information Leaks by User	This data monitor shows the top information leaks of company data by user.	Data Monitor
Last Nation State Concerns	This data monitor shows the latest traffic flagged as a potential concern for the nation state.	Data Monitor
Information Leaks by Destination - Graph	This data monitor shows a graph of information leaks by destination.	Data Monitor
Role Violations by Employee Type - Event Graph	This data monitor shows an event graph of role violations by employee type and actor along with the asset category of the target system.	Data Monitor

Resource	Description	Type
Top Company Information Leaks by Address	This data monitor shows the top information leaks of company data by address.	Data Monitor
Leaked Files by User - Graph	This data monitor shows a graph of leaked files per user.	Data Monitor
Top Information Leaks by Address	This data monitor shows the top information leaks by address.	Data Monitor
Competitive Inbound Email Communication	This data monitor shows events indicating emails from a competitor's email DNS domain.	Data Monitor
Top Information Leaks by Destination User	This data monitor shows the top information leaks by destination user.	Data Monitor
Top Personal Information Leaks by User	This data monitor shows the top information leaks of personal data by user.	Data Monitor
Top Senders to Job Addresses	This data monitor shows the top senders of email to job-related email addresses.	Data Monitor
Scans	This data monitor shows scanning activity.	Data Monitor
Top Failed Email Recipients	This data monitor shows the recipients causing the most errors with their email traffic.	Data Monitor
New Services	This data monitor shows new services that were detected on machines.	Data Monitor
Anomalous Traffic	This data monitor shows anomalous traffic.	Data Monitor
Classification Level Traffic High to Low	This data monitor shows all traffic originating from a higher level classification and targeting a lower level classification.	Data Monitor
Last 10 Company Data Leaks	This data monitor shows the last ten leaks of company data.	Data Monitor
Classification Level Traffic Low to High	This data monitor shows all traffic originating from a lower level classification and targeting a higher level classification.	Data Monitor
Top Personal Information Leaks by Address	This data monitor shows the top information leaks of personal data by address.	Data Monitor
Last 10 Personal Data Leaks	This data monitor shows the last ten leaks of personal data.	Data Monitor
Country of Concern Traffic	This data monitor shows events whose source or destination addresses are from a country of concern as specified on the Countries of Concern active list.	Data Monitor

Resource	Description	Type
Top Rejected Senders	This data monitor shows the top rejected sender addresses.	Data Monitor
Top Files Leaked	This data monitor shows a list of the top files that were leaked.	Data Monitor
Top Job Titles with Suspicious Activity	This data monitor shows the top job titles exhibiting suspicious activity.	Data Monitor
Top Information Leak Policies	This data monitor shows information leak events.	Data Monitor
Competitive Outbound Email Communication	This data monitor shows events indicating emails to a competitor's email DNS domain.	Data Monitor
AttributableActor	This global variable returns all the information for an actor, where the event to actor attribution is done using either attacker or target user name fields, or the source IP address. Note: To turn lookups based on the source IP address, in the Parameters tab, do not use the actorByAccountOrSourceIP local variable to lookup the actor, use the UUID field of the ActorByAccountID global variable instead.	Global Variable
ActorByIP	This global variable returns all the information for an actor, where the event to actor attribution is done using the source IP address.	Global Variable
ActorByAccountID	This global variable maps the account information in an event with an actor. The account information consists of the device vendor and product, and information derived from the attacker or target user name, with preference to the target user name.	Global Variable
ActorFromIPMap	This global variable returns an actor's UUID, full name, username used, and login type if the actor is associated with a source IP address.	Global Variable
ActorByAttackerUserName	This variable maps the account information in an event with an actor. The account information consists of the device vendor, device product, connector address, connector zone, and information derived from the attacker user name.	Global Variable
solnPatternDiscoveryConst	This variable returns a constant string that can be used in Pattern Discovery profiles when it is not required to specify either a Source or a Target event field.	Global Variable
ActorByTargetUserName	This variable maps the account information in an event with an actor. The account information consists of the device vendor, device product, connector address, connector zone, and information derived from the target user name.	Global Variable
solnGetAuthenticator	This global variable extracts the authenticator from the event by looking up the Account Authenticators list using event fields.	Global Variable
solnGetUsername	This global variable returns user name in an event from target user name or attacker user name, with preference to the target user name.	Global Variable
solnTargetAssetGroup	This global variable extracts group name from the URI of the target asset's asset category, assuming the asset category exists in the Network Domains.	Global Variable

Resource	Description	Type
ActorByAccountIDThreatScore	This global variable retrieves an actor's threat score based on the UUID provided by the ActorByAccountID global variable.	Global Variable
AccountIDForLogins	This global variable determines which event username field to use.	Global Variable
ActorByUUID	This Actor global variable looks for a UUID in Device Custom String1, and retrieves the Actor with that UUID.	Global Variable
Email	This field set is used for the active channel showing email traffic.	Field Set
Events with ActorByAccountID	This field set selects the fields appropriate for viewing events correlated with actor and can be customized for the UBM active channels.	Field Set
Events with AttributableActor	This field set selects the fields appropriate for viewing events correlated with either account-id or IP address and can be customized for the UBM active channels.	Field Set
Hacker Tool Web Site	This field set is used for the Hacker Tool Web Site active channel.	Field Set
Events with ActorByUUID	This field set selects the fields appropriate for viewing events correlated with actor and can be customized for the UBM active channels.	Field Set
Information Leak	This field set is used for the Information Leak active channel.	Field Set
Job Hunting FS	This field set is used for the Job Traffic active channel.	Field Set
Role Violations	This field set selects the fields appropriate for viewing events in which an actor accessed a target system for which they do not have the defined role.	Field Set
Scanning	This filter selects events that indicate scanning activity.	Filter
Employee Type - Contractor	This filter selects events attributable to actors having an employee type of contractor.	Filter
Successful Logins	This filter identifies successful logins by both administrative and non-administrative users across a variety of operating systems (Unix, Windows 2003, Windows 2008).	Filter
New Service Detected	This filter selects events indicating that a new service was detected.	Filter
Internal Source	This filter is looking for events coming from inside the company network.	Filter
Information Leak of Company Data from User	This filter selects events indicating improper transmission of company data where the attacker username is not null.	Filter
Suspicious Documents	This filter defines suspicious documents. Add the fileNames of suspicious documents to the condition of this filter to monitor these documents.	Filter
Suspicious Activity	This filter selects events indicating suspicious activity that merits investigation.	Filter
ArcSight Events	This filter selects events in which the Device Vendor and Device Product is ArcSight.	Filter
Proxy Traffic	This filter selects events indicating proxy traffic. Modify this filter to select events that match your environment if needed.	Filter

Resource	Description	Type
Traffic Analysis	This filter selects traffic analysis events such as those from network based anomaly detection systems.	Filter
Physical Access System Events	This filter selects all events from physical access systems.	Filter
ActorByAccountID is NULL	This filter selects events which can not be correlated to an actor based on the attacker or target user name fields.	Filter
ActorByAccountID is NOT NULL	This filter selects events which can be correlated to an actor based on the attacker or target user name fields.	Filter
Information Leak of Company Data	This filter selects events indicating the improper transmission of confidential data where the data was company information.	Filter
Information Leak Events to Address	This filter selects events indicating the improper transmission of confidential data where the target address is not null.	Filter
Blocked Web Page Access	This filter shows blocked Web page access reported generally by proxies.	Filter
Information Leak of Personal Data	This filter selects events indicating the improper transmission of confidential data where the data was personal information.	Filter
Status - Disabled	This filter selects events in which the actor associated with the attacker or target user name in the event has been disabled.	Filter
Rejected Emails	This filter selects events indicating emails which were rejected by the email server.	Filter
Target User Name is NOT NULL	This filter selects events in which the attacker user name field is populated.	Filter
Information Leak Rule Firings	This filter selects UBM information leak correlation events.	Filter
Information Leak Events from User	This filter selects events indicating the improper transmission of confidential data where the attacker username is not null.	Filter
All Login Events to Known Shared Accounts	This filter identifies all login events in which a known shared account is being used. For this filter to work correctly, the Known Shared Accounts active list must be populated with all known shared accounts and their associated applications. This filter will identify successful, failed, and attempted logins.	Filter
Failed Email Communications	This filter selects events that indicate failed email communications.	Filter
Information Leak of Personal Data from Address	This filter selects all information leak events related to personal information where the attacker address is not null.	Filter
Email Traffic	This filter selects events indicating successful email communications.	Filter
Information Leak of Files to Address	This filter selects events indicating improper transmission of files, where the target address is not null.	Filter
New Hire Actors	This filter selects events attributable to actors on the New Hire Actors active list.	Filter
Hacker Tool Website Access	This filter selects base events indicating access to hacker tool websites.	Filter

Resource	Description	Type
Unsuccessful Windows Logins for Valid Username	This filter identifies unsuccessful login events for a valid username recorded on Microsoft Windows domain controllers.	Filter
Role - DBA	This filter selects events attributable to actors having a role of dba.	Filter
Events with Actor	This filter identifies events that can be attributed to an actor either by virtue of the event user name or the originating IP address.	Filter
After Hours	This filter defines the time period of after hours. Change this filter to adjust the default settings.	Filter
Traffic to Competition	This filter selects events destined for competitors' domains.	Filter
Traffic from Competition	This filter selects events coming from competitors' domains.	Filter
Information Leak Events	This filter selects events indicating the improper transmission of confidential data.	Filter
Email To Public Webmail Servers	This filter selects events indicating emails going to public webmail servers such as AOL, Yahoo, or Hotmail.	Filter
Unsuccessful or Attempted Logins	This filter identifies all login events in which the outcome was not a definite success, in other words either a failure or an attempt.	Filter
Classification Level - Higher to Lower	This filter shows traffic from a higher classification level to a lower level.	Filter
ASM Events	This filter selects internal monitoring events involving data monitor resources.	Filter
Confidential Documents	This filter defines confidential documents. Add the fileNames of confidential documents to the condition of this filter to monitor these documents.	Filter
Building Access Events	This filter selects all building access events, such as a user badging into a building.	Filter
Job Hunting	This filter looks for traffic that might indicate possible job hunting activity, including both base events and triggers rules.	Filter
Information Leak Events to User	This filter selects events indicating the improper transmission of confidential data where the target username is not null.	Filter
Privileged Actor Activity	This filter selects events attributable to actors having a privileged role such as administrator or dba.	Filter
Successful Building Access Events	This filter selects successful building access events.	Filter
Emails To Job Addresses	This filter monitors emails being sent to addresses of the form jobs@ or similar forms.	Filter
Printing Activity	This filter selects events indicating printing activity.	Filter
Audit Options Table Delete	This filter selects events indicating that a user has attempted to delete their audit settings directly from the table audit options table.	Filter

Resource	Description	Type
Status - Deleted	This filter selects events in which the actor associated with the attacker or target user name in the event has been disabled.	Filter
All Printing Events	This filter selects events indicating printing activity.	Filter
Traffic to or from Competition	This filter selects events indicating traffic to or from competitors' domains.	Filter
Target User Name is NULL	This filter selects events in which the target user name field is not populated.	Filter
Traffic to Competition - Email	This filter selects events indicating emails sent to a competitor's email DNS domain.	Filter
Role Violations	This filter selects events in which an actor accesses a target system belonging to a department to which they do not belong, and for which they do not have a defined role.	Filter
Target Username is a System Account	This filter selects events in which the target user name is a system account.	Filter
Windows Account Lockouts	This filter defines the event that is generated if a Microsoft Windows user account gets locked out.	Filter
Attacker User Name is a System Account	This filter selects events in which the attacker user name is a system account.	Filter
Traffic from Competition - Email	This filter selects events indicating emails from a competitor's email DNS domain.	Filter
Windows 2008 Authentication Ticket Request	This filter identifies Microsoft Windows 2008 events which indicate that a Kerberos authentication ticket was requested.	Filter
Information Leak of Personal Data from User	This filter selects all information leak events related to personal information where attacker username is not null.	Filter
Information Leak Events from Address	This filter selects events indicating the improper transmission of confidential data where the attacker address is not null.	Filter
Information Leak of Company Data from Address	This filter selects events indicating the improper transmission of confidential data where the data included company information and the attacker address was not null.	Filter
Nation State Concern Traffic	This filter selects traffic that is of concern to nation states. For example, such traffic might include export control violations and terrorist threats.	Filter
Windows 2003 Authentication Ticket Request	This filter identifies Microsoft Windows Kerberos Authentication Ticket Request events. These events are generated when a user logs into an Active Directory domain.	Filter
Audit Table Delete	This filter selects all deletions from the audit table.	Filter
Non-ArcSight Events	This filter selects events in which the Device Vendor and Device Product is not ArcSight.	Filter
Member Added to Privileged Group - Windows 2003	This filter identifies Windows 2003 events that indicate a user has added to a domain local, global or universal security group. These groups are defined in the Privileged User Roles active list.	Filter
Oracle User Added to DBA Role	This filter selects events indicating an Oracle user account was given the role of dba.	Filter

Resource	Description	Type
Printing Resumes	This filter detects printing events in which the documents being printed looks like resumes.	Filter
Login Attempts	This filter selects any attempts at logging into systems. It excludes machine logins into Microsoft Windows systems.	Filter
New Host Detected	This filter selects events indicating that a new host was detected on the network.	Filter
Successful Logins - Unix	This filter identifies successful login attempts to Unix machines.	Filter
Suspicious Activity by Threat Score Actors	This filter selects events indicating suspicious activity from actors whose threat score is greater than zero.	Filter
Windows Events with a Non-Machine User	This filters identified Microsoft Windows events that have a non machine/system user either in the attacker or the target fields.	Filter
Anomalous Connections	This filter selects events indicating anomalous network connections.	Filter
Successful and Unsucessful Logins - Windows 2003	This filter identifies both successful and unsuccessful logins on Windows 2003 domain controller machines.	Filter
Threat Score Contributors	This filter selects rule trigger events that contribute to the Actor Threat Score.	Filter
Employee Type - Part Time	This filter selects events involving users having an employee status type of Part Time.	Filter
Information Leak of Files from User	This filter selects events indicating the improper transmission of files where the attacker username is not null.	Filter
Member Added to Privileged Group - Windows 2008	This filter identifies Windows 2008 events that indicate a user is added to a domain local, global or universal security group. These groups are defined in the Privileged User Roles active list.	Filter
Non-ArcSight Internal	This filter excludes internal ArcSight events.	Filter
Attributable Actor is NULL	This filter selects events which can not be correlated to an actor based on the attacker or target user name fields, or by the attacker address field.	Filter
Traffic to or from Competition - Email	This filter selects events indicating emails to or from a competitor's email DNS domain.	Filter
Information Leak of Files	This filter selects events indicating the improper transmission of confidential data where the file name is not null.	Filter
Countries of Concern Traffic	This filter selects events whose source or destination addresses are from a country of concern as specified on the Countries of Concern active list.	Filter
At Risk Actor	This filter's conditions define the types of actors who might be considered at risk, and who should be monitored at a higher level of scrutiny.	Filter
Member Added to Privileged Group - Windows	This filter selects events indicating a Windows object was added to a privileged group. Privileged groups are defined in the Privileged User Groups active list.	Filter
Audit Log Cleared	This filter selects events indicating that a host audit log was cleared.	Filter

Resource	Description	Type
Successful Logins - Windows 2003	This filter identifies successful login events to Windows 2003 domain controller machines.	Filter
Classification Level - Lower to Higher	This filter shows traffic from a lower classification level to a higher level.	Filter
Attributable Actor is NOT NULL	This filter selects events in which an actor can be attributed to an event either by username or by source IP.	Filter
Database Authentication	This filter selects database authentication events.	Filter
Suspicious Activity by Privileged Actor	This filter selects events indicating suspicious activity from an actor with a privileged role.	Filter
Address or Username Present	This filter checks whether any of attacker address, attacker username, or target username are present in the event.	Filter
ActorByIP is NOT NULL	This filter checks if an actor can be associated with the source IP address of the event.	Filter
Suspicious Activity Rule Firings	This filter selects UBM suspicious activity correlation events.	Filter
Arcsight Internal Events	This filter selects ArcSight ESM internally generated events.	Filter
Failed Building Access Events	This filter selects failed building access events.	Filter
Proxy Event Categorization	This filter selects events indicating proxy traffic. The filter conditions are written considering the categorization of known proxy events.	Filter
Company Concern Traffic	This filter selects suspicious events that are a concern for many organizations. For example, such events might include accessing forbidden Web sites, leaking data, and performing job searches.	Filter
Large Email To Public Webmail Servers	This filter looks for large emails going to Public Webmail servers.	Filter
Disgruntled Actors	This filter selects events attributable to actors on the Disgruntled Actors active list.	Filter
Username Present	This filter checks whether any of attacker username, or target username are present in the event.	Filter
Printing After Hours	This filter selects events that indicate printing activity occurring after hours.	Filter
Unsuccessful Logins for Valid Username - Windows 2008	This filter identifies unsuccessful logins for a valid username on Windows 2008 domain controller machines.	Filter
Actor Threat Score > 0	This filter identifies events from Actors whose threat score is greater than 0.	Filter
Windows Events	This filter selects all events in which the device product field is Microsoft Windows.	Filter
Unsuccessful Logins for Valid Username - Windows 2003	This filter identifies unsuccessful logins for a valid username on Windows 2003 domain controller machines.	Filter
Building Egress Events	This filter selects all building egress events, such as a user badging out of a building.	Filter

Resource	Description	Type
MITRE ATT&CK Activity - Department and MITRE Techniques	Identifies patterns related to MITRE Techniques by Department. By default, patterns will be identified when the same set of three or more MITRE Techniques and Triggered rules of at least two different departments.	Profile
MITRE ATT&CK Activity - Users and MITRE Techniques	Identifies patterns related to MITRE Techniques by users. By default, patterns will be identified when the same set of three or more MITRE Techniques and Triggered rules of at least two different users.	Profile
Removable Media - Hostname to Media	Identifies patterns in removable media activity. By default, patterns will be identified when the set of two or more media and host involved on data transfer of at least two files.	Profile
Suspicious Activity	This profile helps detect patterns of suspicious activity across actors.	Profile
Suspicious Activity Rule Firings	This profile detects patterns of suspicious activity rules triggered across actors.	Profile
Failed Database Authentication Review	This query returns all failed authentications to databases.	Query
Role Violations Detail for Target Asset Role	This query selects information about the actor, target host, device and count of events in which the user does not have the proper role to access assets belonging to the specified category.	Query
Resumes Emailed	This query returns events indicating that a resume was emailed.	Query
Role Violations Detail for Employee Type	This query selects information about the actor, target asset, device and count of events in which the user does not have the proper role to access the asset for actors belonging to the specified employee type.	Query
Privileges Granted without Proper Role - Oracle	This query returns events indicating that an Oracle account belonging to a non-dba actor was given the role of dba.	Query
Role Violations Summary for Employee Type	This query returns the actor's full name, target asset categories, and the number of role violations for the specified employee type.	Query
Oracle NOAUDIT	This query returns all the users for whom auditing has been disabled.	Query
Oracle Privilege Grants	This query returns privileges granted in Oracle.	Query
Top Actors with Suspicious Activity Rule Firings	This query gets the top actors by number of UBM suspicious activity correlation events.	Query
Oracle Users Created	This query returns the new users that have been created within Oracle.	Query
All Suspicious Activity for Role	This query selects the actor's full name, unique ID, vendor, product, event name, and count of all events that can be correlated to an actor having the specified role.	Query
Information Leak - Top Rule Firings	This query returns the top information leak rules triggered.	Query
Suspicious Activity Rule Firings	This query selects correlation events for UBM suspicious activity rules.	Query
Printing Activity After Hours	This query returns events indicating after-hours printing activity.	Query

Resource	Description	Type
Suspicious Activity Rule Firings for Role	This query gets information about UBM suspicious activity correlation events for the specified role.	Query
Top Job Titles with Suspicious Activity Rule Firings	This query gets the top job titles by number of UBM suspicious activity correlation events.	Query
Rejected Email Senders	This query returns the sender, relay, and time of rejected email events.	Query
Suspicious Activity by Threat Score Actors	This query selects information from suspicious events attributed to actors having a threat score greater than zero.	Query
DBA_USERS DELETES	This query selects all DELETE operations on the dba_users table in Oracle.	Query
All Actions for Actor	This query gets aggregated information about events that might be attributable to actors.	Query
All Suspicious Activity	This query selects information from all suspicious events that can be correlated to an actor.	Query
Activity from Disabled Actors	This query returns information from events in which the actor associated with the attacker or target user name in the event has been disabled.	Query
All Suspicious Activity for Employee Type	This query selects the actor's full name, unique ID, vendor, product, event name, and count of all suspicious events that can be correlated to an actor having the specified employee type.	Query
Suspicious Activity Rule Firings for Job Title	This query gets information about UBM suspicious activity correlation events for the specified job title.	Query
Files Emailed	This query returns all files that have been emailed.	Query
Top Threat Score Contributors by Number of Rule Firings	This query identifies the top rules that contribute to actor threat scores, by the total number of times each rule triggered.	Query
Role Violations Detail by Employee Type	This query selects information regarding the actor, target asset and count of events in which the user does not have the proper role to access the asset.	Query
Printing Suspicious Documents	This query returns events indicating printing of suspicious documents.	Query
Role Violations Summary by Employee Type	This query selects the actor's employee type, target asset categories, and count of events in which the user does not have the proper role to access the asset.	Query
Role Violations Summary by Department	This query selects the actor's department, target asset categories, and count of events in which the user does not have the proper role to access the asset.	Query
Top Departments with Suspicious Activity Rule Firings	This query gets the top departments by number of UBM suspicious activity correlation events.	Query
Database Table Access Review	This query returns all database tables that have been accessed and the users accessing them.	Query
Suspicious New Hire Activity	This query selects suspicious events from actors on the New Hire active list.	Query
Failed Building Access Events	This query returns events indicating failed building access.	Query

Resource	Description	Type
Role Violations Detail by Target Asset Role	This query selects information regarding the actor, target asset and count of events in which the user does not have the proper role to access the asset.	Query
Role Violations Summary for Department	This query returns the actor's full name, target asset categories, and number of role violations for the specified department.	Query
Role Violations Detail for Department	This query selects information regarding the actor, target asset, device and count of events in which the user does not have the proper role to access the asset for actors belonging to the specified department.	Query
Audit Table Delete	This report shows all deletions from the audit table.	Query
Suspicious Activity Rule Firings for Actor	This query gets information about UBM suspicious activity correlation events for the specified actor.	Query
Audit Options Table Delete	This query selects any user attempting to delete their audit settings directly from the table audit options table.	Query
Suspicious Notice-Given Actor Activity	This query selects suspicious events by actors on the Notice Given list.	Query
Role Violations Summary for Target Asset Role	This query returns the number of role violations per user and target asset for the specified target asset category.	Query
Role Violations Summary by Target Asset Role	This query selects target asset categories, target host name and count of events in which the user does not have the proper role to access the asset.	Query
Oracle Grant Role DBA	This query returns all successful dba role grants by the user who executed the grant.	Query
DBA_USERS Access	This query returns all SELECT operations on the dba_users table in Oracle.	Query
Suspicious Activity Rule Firings for Employee Type	This query gets information about UBM suspicious activity correlation events for the specified employee type.	Query
DBA_USERS UPDATES	This query returns all updates to the dba_users table in Oracle.	Query
After Hours Database Accesses	This query selects events indicating after hours database access.	Query
Threat Score Contributors - Trend	This query gets aggregated information about correlation events for rules that contribute to an actor's threat score.	Query
Specific Document Printed	This query returns events indicating that the specified document has been printed.	Query
Suspicious Disgruntled User Activity	This query selects suspicious events by actors on the Disgruntled list.	Query
Suspicious Activity by Privileged Actors	This query returns information from events indicating suspicious activity from an actor having a privileged role.	Query
Specific Document Transferred	This query returns events indicating that the specified document was transferred.	Query
Role Violations Detail by Department	This query selects information regarding the actor, target asset and count of events in which the user does not have the proper role to access the asset.	Query

Resource	Description	Type
Traffic to Competition	This query returns all communication with competitive organizations as defined by the asset categories or the Competition active list.	Query
Suspicious Document Transferred	This query returns events indicating that a suspicious document has been transferred.	Query
Traffic to Countries of Concern	This query returns all communication with countries of concern as defined by the Countries of Concern active list.	Query
Suspicious Activity Rule Firings for Department	This query gets information about UBM suspicious activity correlation events for the specified department.	Query
Privileges Granted without Proper Role - Windows	This query returns events indicating that an account belonging to a non-privileged actor was added to a privileged NT security group.	Query
Database Authentication Review	This query returns all successful database authentications.	Query
All Suspicious Activity for Department	This query selects the actor full name, unique ID, vendor, product, event name, and count of all suspicious events that can be correlated to an actor belonging to the specified department.	Query
Confidential Document To Competition	This query returns users who have sent a confidential document to a competitor.	Query
IP Address to Actor Map	This session list tracks the IP addresses that can be associated with actors. Typically, these IP addresses will belong to single-user machines.	Session List
All Actions for Actor	This hourly trend collects aggregated information about events that might be attributable to actors.	Trend
Threat Score Contributors	This trend captures a summary of all rules that trigger and contribute to the threat scores of actors.	Trend

User Activity Monitoring Use Case

The User Activity Monitoring use case contains resources designed to enable analysts to monitor the activity of users on the network. Many resources break down activity by actors' employee type, department, or other attributes.

By correlating events to an actor and its attributes, analysts, auditors, and managers can monitor and generate activity reports on a per department/employee type/role basis. For example, using this resources in the use case, the following reports can be generated:

- A report showing all the events that were correlated with users that are in the Engineering department.
- A report showing all the events that were correlated with users that are contractors.

- A report showing all the events that were correlated with users that have a role of administrator.
- A report showing all the all activity for a specific actor.

The use case distinguishes between server login activity, application login activity, and activity within applications so that they can be reported on and tracked separately.

The resources provided in the User Activity Reporting use case enable analysts, auditors, and managers to provide the following services:

- Monitoring and reporting on all activity that can be correlated to a specific actor
- Resources that monitor actor activity are based on the All Actions for Actor trend. This trend collects aggregated information about events which might be attributable to actors.
- Monitoring and reporting on all activity on a per department, role, or employee type basis
- Visualizing login activity to applications and servers by department, role, and employee type
- Creating reports to model activity by department, role, and employee type
- Monitoring and reporting on failed/successful login activity by department, role, employee type
- Comparing hourly login activity for a particular actor to the averages for a particular role
- Monitoring and reporting on printing and email activity by actor
- Monitoring and reporting on short term and long term proxy usage
- Reports and query viewers that monitor short term and long term proxy usage are based on the Weekly Proxy Activity and Proxy Activity trends.
- Monitoring and reporting on the physical access of actors (both entering and exiting buildings)
- Reports and query viewers that monitor building access and egress (exiting) events are based on the Building Access and Egress trend.

Configure Resources

Configure the following types of resources for this use case:

- Active List
- Filters
- Rules
- Trends

Active List

Configure the active list listed in the following table. This active list is available from the following location:

`ArcSight Solutions/UBM/User Activity Monitoring`

Populate User Activity Monitoring Active List

Active List	Description	Configuration
My DNS Domains	This active list is used to define the DNS domain names which are owned by the organization.	Configure with all the case sensitive variations of the email DNS domain names used in your organization, for example: • MyCompany.com • mycompany.com • MYCOMPANY.COM

Filters

Configure the following filters for this use case:

- **Authorization Changes/Oracle User Added to DBA Role** filter—Configure this filter to reflect your environment. Add any additional Oracle administrator roles for the filter to track. By default, the role of DBA is specified. To specify an additional role, add an additional File Name condition.
- **User Investigation/All Events from Actor** filter—Specify the Full Name of the actor you want to track as defined by the Full Name attribute of the actor.

Verify that the following filters detect appropriate proxy events in your environment:

- Proxy Traffic
- Successful Web Page Access

Rules

The following rules can be configured for this use case:

- Enable the Add Actor to Badged In List rule if you want to track building access.

By default, all the following actions of this rule are enabled:

- **Add to Active List**—Adds the actor to the Badged In Actors active list.
- **Set Event Field Actions**—Sets field values for the event generated by this rule.

Enable the Actor Changes rule if you want to track building egress.

By default, all the following actions of this rule are enabled:

- **Remove From Active List**—Removes the actor to the Badged In Actors active list.
- **Set Event Field Actions**—Sets field values for the event generated by this rule.

Enable the Add to Daily Active and Remove from Pending Stale rule if you want to track stale accounts.

By default, all the following actions of this rule are enabled:

- **Add to Active List**—Adds the actor to the Daily Active Accounts active list.
- **Remove from Active List**—Removes the actor to the Pending Stale Accounts active list.
- **Set Event Field Actions**—Sets field values for the event generated by this rule.

Enable the Add to Pending Stale rule if you want to track stale accounts.

By default, all the following actions of this rule are enabled:

- **Add to Active List**—Adds the actor to the Actor Changes active list.
- **Set Event Field Actions**—Sets field values for the event generated by this rule.

Enable the Stale Account Detected rule if you want to track stale accounts.

By default, all the following actions of this rule are enabled:

- **Add to Active List**—Adds the actor to the Actor Changes active list.
- **Set Event Field Actions**—Sets field values for the event generated by this rule.

Trends

Reports and query viewers in this use case are based on the trends listed below. Before enabling these trends, verify that these trends collect the expected events for your environment. In addition, you might want to customize the trend before enabling.

Enable the following trends to track proxy activity:

- Weekly Proxy Activity
- Proxy Activity

Enable the All Actions for Actor trend to track events that might be attributable to actors. Enable the Building Access and Egress trend to track building access and egress (exit) events.

Build FlexConnector(s) for Physical Access Devices

The UBM solution contains use cases that make use of feeds from physical access systems, such as badge readers. This process is only required if you want to activate the UBM solution content that leverages feeds from physical

access systems. If you do not complete this process, the content that leverages feeds from physical access systems will remain dormant.

To enable these use cases, develop a FlexConnector according to the instructions in the ArcSight FlexConnector Developer's Guide with the following field mappings to map the key event data into the ArcSight event schema:

ArcSight Field	Physical Access System Value
deviceEventClassId	Unique value for event type used for categorization
deviceReceiptTime	Access Time
destinationUserId	Users badge Id
deviceCustomString1	Location Accessed / Building

Use the following event categories for the following event types:

Event type	Object	Behavior	Technique	Device Group	Outcome	Significance
Successful building access	/Location	/Authentication/Verify		/Physical Access System	/Success	/Normal
Building access rejected	/Location	/Authentication/Verify		/Physical Access System	/Failure	/Information/Warning
Badge-out (someone is leaving a building) [not all badge reader systems support this]	/Location	/Access/Stop		/Physical Access System	/Success	/Normal
Account created/deleted/modified - [Success assumed; in case of a failure, the Outcome needs to reflect that and the significance is /Informational/Error]	/Actor/User	/Authentication/ [Add|Delete|Modify		/Physical Access System	/Success	/Informational
Giving someone access to another room/building - [Success assumed; in case of a failure, the Outcome needs to reflect that and the significance is /Informational/Error]	/Actor/User	/Authorization/Modify		/Physical Access System	/Success	/Informational
Granting access to a room/building for an entire group of users	/Actor/Group	/Authorization/Modify		/Physical Access System	/Success	/Informational

You can add more user context to the events generated by your badge reader by creating a connector event mappings file. For more information, see ArcSight FlexConnector Developer's Guide.

In addition, an entry for the badge ID must be added to the Account Attributes table for each actor. An entry for the FlexConnector must be also added to the Account Authenticators active list with the badge system as the authenticator.

Devices

The following device types can supply events to this use case:

- Intrusion Detection System
- Intrusion Prevention System
- Network Based Anomaly Detection
- Database
- Operating Systems
- Firewalls
- Virtual Private Networks
- Vulnerability Assessment
- Identity Management System
- Policy Management
- Network Equipment
- Content Security, Web Filtering
- Antivirus
- Wireless
- Application

All the devices listed above can supply events to this use case but the resources will only process events from devices, when the device generates events that can be attributed to specific actors.

Resources

The following table lists all the resources explicitly assigned to this use case and any dependent resources. Each resource can be accessed from the User Activity Monitoring use case landing page: /All Use Cases/ArcSight Solutions/UBM/Actor Management, or their URI, for example: /All <Resource Type>/ArcSight Solutions/UBM/<Use Case>/<Resource Name>.

Resource	Description	Type
Monitor Resources		
Activity - Contractor	This active channel shows events attributable to actors having an employee type of contractor.	Active Channel
Remote Login Events	Displays Microsoft Windows 4624 events where the Logon Type is 10. Logon Type 10 is when a user logs on to a computer remotely using Terminal Services or Remote Desktop.	Active Channel
Activity - Full Time Employee	This active channel shows events attributable to actors having an employee type of Full Time.	Active Channel
Physical Access System Events	This active channel shows events generated by physical access systems.	Active Channel
Database Activity	This active channel shows all database activity.	Active Channel
Activity - DBA	This filter selects events attributable to actors having a role of dba.	Active Channel
Activity - Part Time Employee	This active channel shows events attributable to actors having an employee type of Full Time.	Active Channel
All Login Events	This active channel shows login events to servers and applications.	Active Channel
Email Traffic	This active channel shows events generated due to email traffic.	Active Channel
Proxy Traffic	This active channel shows events generated due to proxy traffic.	Active Channel
Printing Activity	This active channel shows all printing activity.	Active Channel
All Events from Specified Actor	This active channel shows all events that can be correlated to a specific actor.	Active Channel
Printing Activity	This dashboard shows all printing activity.	Dashboard
Login Activity by Employee Type	This dashboard shows event graphs of login activity to applications and servers by employee type.	Dashboard
Top Email Communicators	This dashboard shows the top entities involved in email traffic.	Dashboard
Proxy Traffic	This dashboard shows various pieces of information about proxy traffic.	Dashboard
Badged In Actors	This dashboard shows information regarding actors that are currently badged in.	Dashboard
Email Relays	This dashboard shows information related to email relays.	Dashboard

Resource	Description	Type
User Authorization Changes	This dashboard summarizes user authorization changes, such as group membership and privilege assignments in operating systems and applications.	Dashboard
Bandwidth Usage	This dashboard shows bandwidth usage information for actors.	Dashboard
Login Activity by Department	This dashboard shows event graphs of login activity to applications and servers by department.	Dashboard
Email Graphs	This dashboard shows email traffic graphs.	Dashboard
Database Activity	This dashboard shows database related activity.	Dashboard
All Activity for Known Actors	This query viewer shows all events that can be attributed to any actor in the system.	Query Viewer
Top Countries with Badged In Actors	This query viewer shows the top countries that have the most number of successful building access events.	Query Viewer
Pending Stale Accounts	This query viewer shows a list of pending stale account IDs with the associated actor and device information.	Query Viewer
Uncommon Websites	This query viewer shows those websites that were accessed by few actors.	Query Viewer
Actors by Account ID - Websites Accessed	This query viewer shows websites accessed by actors who were derived from the base events by virtue of their account IDs.	Query Viewer
Stale Accounts	This query viewer shows a list of stale account IDs with the associated actor and device information.	Query Viewer
Total Number of Badged In Actors	This query viewer shows the total number of currently badged in actors.	Query Viewer
Badged In Actor Details	This query viewer shows relevant actor base attribute information for those actors that are currently badged in.	Query Viewer
Top Bandwidth - Download - by IP	This query viewer shows the top actors that have the most number of bytes downloaded via proxy servers. The actors are derived by virtue of the event source IP address.	Query Viewer
Top Departments with Badged In Actors	This query viewer shows the top departments that have the most number of successful building access events.	Query Viewer
Top Bandwidth - Upload - by IP	This query viewer shows the top actors that have the most number of bytes uploaded via proxy servers. The actors are derived from by virtue of the event source IP address.	Query Viewer
Top Bandwidth - Upload - by Account ID	This query viewer shows the top actors that have the most number of bytes uploaded via proxy servers. The actors are derived by virtue of their account IDs.	Query Viewer
Actor By IP - Websites Accessed	This query viewer shows websites accessed by actors who were derived from the base events by virtue of the event source IP address.	Query Viewer
Top Bandwidth - Download - by Account ID	This query viewer shows the top actors that have the most number of bytes downloaded via proxy servers. The actors are derived by virtue of their account IDs.	Query Viewer

Resource	Description	Type
Top Roles with Badged In Actors	This query viewer shows the top roles that have the most number of successful building access events. For a role to be selected at least two actors must have the same role.	Query Viewer
Top Actors Badging In	This query viewer shows those actors that have the most number of successful building access events.	Query Viewer
Daily Active Accounts	This query viewer shows a list of pending stale account IDs with the associated actor and device information.	Query Viewer
Top Badged In Locations	This query viewer shows the top locations that have the most number of successful building access events.	Query Viewer
Successful Server Logins for Employee Type	This report shows a stacked bar chart of successful server logins by user for a given employee type. A table is also included. Enter the employee type parameter at runtime to restrict the report to users of a certain employee type, such as Full Time.	Report
Printing Volume in Pages Review	This report shows printing volume in pages by user.	Report
Top Blocked Actors by Account ID	This report shows the top actors by number of events and data transferred that have requests blocked by proxy servers. The actors are derived by virtue of their account IDs.	Report
Top Email Senders (Size)	This report shows the top email senders based on the size of emails sent.	Report
Successful Server Logins for Role	This report shows a stacked bar chart of server logins by user for a given role. A table is also included. Enter the role parameter at runtime to restrict the report to users with a certain role, such as Developers.	Report
Physical Access System Events Over the Past Day	This report shows a count of building access and egress events per hour over the past day.	Report
Websites Accessed by Actor - Month	This report shows all the websites visited by the specific actor over the past month.	Report
Top Blocked Actors by IP	This query selects the top actors by number of events and data transferred that have requests blocked by proxy servers. The actors are derived by virtue of the event source IP address.	Report
Failed Server Logins for Department	This report shows a stacked bar chart of failed server logins by user for a given department. A table is also included. Enter the department parameter at runtime to restrict the report to users in a certain department, such as Engineering.	Report
Top Email Receivers (Amount)	This report shows the top email recipients based on number of emails received.	Report
Top Accessed Websites (Size)	This report shows the top accessed web sites by data transferred.	Report
Activity Based Modeling by Employee Type	This report shows the asset categories, vendors, and applications accessed by employees of each employee type.	Report
Failed Server Logins for Employee Type	This report shows a stacked bar chart of failed server logins by user for a given employee type. A table is also included. Enter the employee type parameter at runtime to restrict the report to users of a certain employee type, such as Full Time.	Report

Resource	Description	Type
Successful Application Logins for Employee Type	This report shows a stacked bar chart of successful application logins by user for a given employee type. A table is also included. Enter the employee type parameter at runtime to restrict the report to users of a certain employee type, such as Full Time.	Report
Top Accessed Websites	This report shows the top accessed websites by number of events.	Report
SU and SUDO Activity	This report shows activity related to su or sudo on UNIX machines. The attackerUser is trying to execute code with the privileges of the targetUser.	Report
Activity Based Modeling by Role	This report shows the asset categories, vendors, and applications accessed by employees of each combination of roles.	Report
All Activity for Employee Type	This report shows the actor full name, vendor, product, event name, and count of all events that can be correlated to an actor having the specified employee type.	Report
Failed Application Logins for Department	This report shows a stacked bar chart of failed application logins by user for a given department. A table is also included. Enter the department parameter at runtime to restrict the report to users in a certain department, such as Engineering.	Report
UBM - Case Chart	This report shows a count of cases per operational impact and stage.	Report
All UBM Cases	This report shows all cases in the UBM case group.	Report
Top Proxy Users (Size)	This report shows the top users accessing web pages by data transferred.	Report
All Activity for Known Actors	This report shows all events that can be attributed to any actor in the system.	Report
All Activity for Specific Actor	This report shows a summary of all activity that can be attributed to the specified actor.	Report
Failed Application Logins for Role	This report shows a stacked bar chart of failed application logins by user for a given role. A table is also included. Enter the role parameter at runtime to restrict the report to users with a certain role, such as Developers.	Report
Websites Accessed by Actor - Day	This report shows all the websites visited by the specific actor over the past day.	Report
Physical Access System Events for Actor	This report shows building access and egress events for the specified actor.	Report
UBM - Top Rule Firings	This report shows the rules that trigger the most in the UBM solution.	Report
Successful Server Logins for Department	This report shows a stacked bar chart of successful server logins by user for a given department. A table is also included. Enter the department parameter at runtime to restrict the report to users in a certain department, such as Engineering.	Report
UBM - Open Cases	This report shows the current status of all open UBM cases	Report
Successful Application Logins for Department	This report shows a stacked bar chart of successful application logins by user for a given department. A table is also included. Enter the department parameter at runtime to restrict the report to users in a certain department, such as Engineering.	Report

Resource	Description	Type
All Activity for Department	This report shows the actor full name, vendor, product, event name, and count of all events that can be correlated to an actor belonging to the specified department.	Report
Top Email Senders (Amount)	This report shows the top email senders based on the number of emails sent.	Report
Top Blocked Websites (Size)	This report shows the top websites blocked by proxy servers by data transferred.	Report
Top Email Receivers (Size)	This report shows the top email recipients based on the size of emails received.	Report
Successful Application Logins for Role	This report shows a stacked bar chart of successful application logins by user for a given role. A table is also included. Enter the role parameter at runtime to restrict the report to users with a certain role, such as Developers.	Report
Activity Based Modeling by Department	This report shows the asset categories, vendors, and applications accessed by employees in each department.	Report
Physical Access System Events for Department	This report shows building access and egress events for the specified department.	Report
All Activity for Role	This report shows the actor full name, vendor, product, event name, and count of all events that can be correlated to an actor having the specified role.	Report
Top Proxy Users	This report shows the top users accessing web pages by number of events	Report
Printing Activity for Specific Actor	This report shows all printing activity for the specified actor.	Report
Failed Application Logins for Employee Type	This report shows a stacked bar chart of failed application logins by user for a given employee type. A table is also included. Enter the employee type parameter at runtime to restrict the report to users of a certain employee type, such as Full Time.	Report
Authorization Changes for Department	This report shows events indicating authorization changes within applications. The events are limited to actors within the specified department.	Report
Physical Access System Events	This report shows successful building access events.	Report
Authorization Changes	This report shows events indicating authorization changes within applications.	Report
Failed Server Logins for Role	This report shows a stacked bar chart of failed server logins by user for a given role. A table is also included. Enter the role parameter at runtime to restrict the report to users with a certain role, such as Developers.	Report
Printing Volume in Bytes Review	This report shows printing volume in bytes by user.	Report
Hourly Login Averages for User vs. Role	This report compares a given user's login activity to servers and applications compared to a given role.	Report
URLs Accessed	This report shows the accessed URLs for a specified period of time.	Report
Top Largest Emails	This report shows the largest emails that have been sent.	Report

Resource	Description	Type
Top Blocked Websites	This report shows the top websites blocked by proxy servers by the number of requests blocked.	Report
Physical Access System Events Over the Past Week	This report shows a count of building access and egress events per day over the past week.	Report
Stale Accounts	This report shows the accounts on the Stale Accounts active list.	Report
After Hours Building Accesses	This report shows events indicating after hours building access.	Report
Library - Correlation Resources		
Remove Actor from Badged In List	This rule detects when someone leaves a building and removes the actor's full name from the badged in actors active list.	Rule
Pass-the-Hash Attack Detected T1550.002	Detects if Pass-the-Hash (PtH) attack detected.	Rule
Potential Data Theft Through Removable Media across Multiple Machines T1052.001	Detects possible data exfiltration from the same actor across multiple machines.	Rule
Possible Data Theft Through Removable Media from the Same Machine T1052.001	Detects possible data exfiltration via removable media from the same actor on a specific machine.	Rule
Add Actor to Badged In List	This rule detects successful building access and adds the actor's full name to the badged in actors active list	Rule
Add to Pending Stale	This rule triggers when an account expires off of the Daily Active Accounts active list, indicating it has not been logged into in 24 hours since the previous login. The rule adds the account information to the Pending Stale Accounts active list.	Rule
Add to Daily Active and Remove from Pending Stale	This rule triggers when a user successfully authenticates to an application, and adds pertinent information from the event to the Daily Active Accounts active list. It will not trigger if a user is already in the list.	Rule
Stale Account Detected	This rule triggers on events indicating that a user has expired from the Pending Stale Accounts active list, indicating the account has not been used in 6 months. The rule adds the account information to the Stale Accounts active list.	Rule
Library Resources		
My DNS Domains	This active list defines the DNS domain names which are owned by the organization.	Active List
Badged In Actors	This active list maintains a list of actors who have badged into the building. By default, actors expire from the list in 1 day.	Active List

Resource	Description	Type
Account Authenticators	This active list is used by the actor global variables to determine what the Identity Management authenticator is, base on the event, so that an actor can be determined from event information.	Active List
Pending Stale Accounts	This active list maintains relevant information about accounts that have not been used since they expired off of the Daily Active Accounts active list. Accounts will remain in this list for 6 months unless the account is used, when it will be removed from the list.	Active List
Stale Accounts	This active list contains the accounts that have expired off of the Pending Stale Accounts active list, indicating they have not been used in over 6 months.	Active List
Daily Active Accounts	This active list keeps a list of relevant information about actors with active accounts. The default expiration is one day.	Active List
Servers	This is a solutions asset category.	Asset Category
Network Domains	This is a solutions asset category.	Asset Category
Last Users Printing Resumes	This data monitor shows the last users printing resumes.	Data Monitor
Server Logins by Department - Event Graph	This data monitor shows an event graph of server logins grouped by the actors departments.	Data Monitor
Top Outbound Email Recipients	This data monitor shows the top recipients of outbound email.	Data Monitor
Top Printing Users	This data monitor shows the users with the most printing activity.	Data Monitor
Outbound Email	This data monitor shows outbound email traffic.	Data Monitor
Top Outbound Email Senders	This data monitor shows the top actors sending emails to external addresses.	Data Monitor
Top Blocked Web Pages	This data monitor shows the top Web pages blocked by proxies.	Data Monitor
Database Table Access - Graph	This data monitor shows a graph of database table access.	Data Monitor
Top Relays Incoming	This data monitor shows the top 10 relays that were used by for sending incoming email.	Data Monitor
User Privilege Added or Revoked - Event Graph	This data monitor creates an event graph of events indicating a specific privilege was added or revoked. The application, privilege, and actor are included in the graph.	Data Monitor
Inbound Email	This data monitor shows inbound email traffic.	Data Monitor

Resource	Description	Type
Top Traffic by Source	This data monitor shows the actors with the most traffic registered by proxies.	Data Monitor
User Group Membership Changed - Event Graph	This data monitor creates an event graph of events indicating a user group membership change within an application. The application, group, and actor are included in the graph.	Data Monitor
Last Users Printing After Hours	This data monitor shows the last users that printed after hours.	Data Monitor
Application Logins by Department - Event Graph	This data monitor shows an event graph of application logins from users and their departments.	Data Monitor
Top Relays Outgoing	This data monitor shows the top 10 relays that were used by for sending outgoing email.	Data Monitor
Top Inbound Email Recipients	This data monitor shows the top actors receiving inbound email.	Data Monitor
Server Logins by Employee Type - Event Graph	This data monitor shows an event graph of server logins from users and their employee type.	Data Monitor
Top Accessed Web Pages	This data monitor shows the top accessed Web pages.	Data Monitor
Database Access - Graph	This data monitor shows a graph of database machine access.	Data Monitor
Application Logins by Employee Type - Event Graph	This data monitor shows an event graph of application logins from users and their employee type.	Data Monitor
Top Inbound Email Senders	This data monitor shows the top senders of inbound email traffic.	Data Monitor
Top Blocked Sources	This data monitor shows the top actors blocked by proxies.	Data Monitor
AttributableActor	This global variable returns all the information for an actor, where the event to actor attribution is done using either attacker or target user name fields, or the source IP address. Note: To turn lookups based on the source IP address, in the Parameters tab, do not use the actorByAccountOrSourceIP local variable to lookup the actor, use the UUID field of the ActorByAccountID global variable instead.	Global Variable
solnGetAuthenticator	This global variable extracts the authenticator from the event by looking up the Account Authenticators list using event fields.	Global Variable
ActorByIP	This global variable returns all the information for an actor, where the event to actor attribution is done using the source IP address.	Global Variable
solnGetUsername	This global variable returns user name in an event from target user name or attacker user name, with preference to the target user name.	Global Variable

Resource	Description	Type
ActorByAccountID	This global variable maps the account information in an event with an actor. The account information consists of the device vendor and product, and information derived from the attacker or target user name, with preference to the target user name.	Global Variable
ActorFromIPMap	This global variable returns an actor's UUID, full name, username used, and login type if the actor is associated with a source IP address.	Global Variable
solnGetPhysicalAccessEvent	This global variable returns whether a successful badge in or badge out event occurred for physical access events.	Global Variable
solnPatternDiscoveryConst	This variable returns a constant string that can be used in Pattern Discovery profiles when it is not required to specify either a Source or a Target event field.	Global Variable
ActorByAttackerUserName	This variable maps the account information in an event with an actor. The account information consists of the device vendor, device product, connector address, connector zone, and information derived from the attacker user name.	Global Variable
AccountIDForLogins	This global variable determines which event username field to use.	Global Variable
ActorByTargetUserName	This variable maps the account information in an event with an actor. The account information consists of the device vendor, device product, connector address, connector zone, and information derived from the target user name.	Global Variable
Group Membership Changed	This field set selects the fields appropriate for viewing events indicating user group membership changes within an application.	Field Set
Physical Access System Events	This field set selects the fields appropriate for viewing physical access system events correlated with actor.	Field Set
Email	This field set is used for the active channel showing email traffic.	Field Set
Events with ActorByAccountID	This field set selects the fields appropriate for viewing events correlated with actor and can be customized for the UBM active channels.	Field Set
Printing	This field set is used for the printing activity active channel.	Field Set
Privilege Added or Revoked	This field set selects the fields appropriate for viewing events indicating a specific privilege was added or revoked.	Field Set
Proxy	This field set is used for the active channel showing proxy traffic.	Field Set
Remote Logon Activity	Contains fields required to monitor remote logon activity.	Field Set
Database Activity	This field set selects the fields appropriate for viewing database activity.	Field Set
Remote Desktop Logon Events	Captures Microsoft Windows 4624 events where the Logon Type is 10. Logon Type 10 is when a user logs on to a computer remotely using Terminal Services or Remote Desktop.	Filter
Employee Type - Contractor	This filter selects events attributable to actors having an employee type of contractor.	Filter

Resource	Description	Type
Successful Logins	This filter identifies successful logins by both administrative and non-administrative users across a variety of operating systems (Unix, Windows 2003, Windows 2008).	Filter
Target Username is a System Account	This filter selects events in which the target user name is a system account.	Filter
Actor and Address Present	This filter identifies events where an actor can be attributed to the event as well and both the attacker and target addresses are present.	Filter
Successful Logins - Non-Windows and Non-Unix	This filter selects login events that cannot be attributed to either Microsoft Windows or Unix.	Filter
User Expired from Daily Active Accounts List	This filter selects events indicating an actor has expired from the Daily Active Accounts active list. This means that the actor has not logged in within 24 hours of their last login.	Filter
Attacker User Name is a System Account	This filter selects events in which the attacker user name is a system account.	Filter
ArcSight Events	This filter selects events in which the Device Vendor and Device Product is ArcSight.	Filter
Outbound Email	This filter selects events indicating email traffic from internal domains to external domains.	Filter
Windows 2008 Authentication Ticket Request	This filter identifies Microsoft Windows 2008 events which indicate that a Kerberos authentication ticket was requested.	Filter
Successful Logins - Server	This filter selects events indicating successful logins to servers.	Filter
Proxy Traffic	This filter selects events indicating proxy traffic. Modify this filter to select events that match your environment if needed.	Filter
ActorByAccountID is NULL	This filter selects events which can not be correlated to an actor based on the attacker or target user name fields.	Filter
Inbound Email	This filter selects events indicating email traffic from external domains to internal domains.	Filter
Physical Access System Events	This filter selects all events from physical access systems.	Filter
ActorByAccountID is NOT NULL	This filter selects events which can be correlated to an actor based on the attacker or target user name fields.	Filter
Windows 2003 Authentication Ticket Request	This filter identifies Microsoft Windows Kerberos Authentication Ticket Request events. These events are generated when a user logs into an Active Directory domain.	Filter
Non-ArcSight Events	This filter selects events in which the Device Vendor and Device Product is not ArcSight.	Filter
All Events from Actor	This filter selects all events that can be attributed to the actor specified in the filter conditions.	Filter
Failed Database Authentication	This filter selects all failed database authentications.	Filter

Resource	Description	Type
User Privilege Added	This filter selects events indicating that new rights were assigned to a user.	Filter
SU activity	This filter selects events indicating that someone is executing a su or executing a command under another user account (sudo)	Filter
Blocked Web Page Access	This filter shows blocked Web page access reported generally by proxies.	Filter
Rejected Emails	This filter selects events indicating emails which were rejected by the email server.	Filter
Attacker and Target User NOT SYSTEM	This filter excludes events in which both the attacker and target user name are system or admin accounts, or one is a system account and the other is NULL.	Filter
Oracle User Added to DBA Role	This filter selects events indicating an Oracle user account was given the role of dba.	Filter
Printing Resumes	This filter detects printing events in which the documents being printed looks like resumes.	Filter
Target User Name is NOT NULL	This filter selects events in which the attacker user name field is populated.	Filter
Login Attempts	This filter selects any attempts at logging into systems. It excludes machine logins into Microsoft Windows systems.	Filter
Successful Logins - Unix	This filter identifies successful login attempts to Unix machines.	Filter
Successful Logins - Application - Actor NOT NULL	This filter selects events indicating successful logins to servers where the actor can be derived from the event.	Filter
Successful Logouts - Application	This filter selects events indicating successful application logouts.	Filter
Successful Building Egress Events	This filter selects successful building egress events.	Filter
Windows Events with a Non-Machine User	This filters identified Microsoft Windows events that have a non machine/system user either in the attacker or the target fields.	Filter
Failed Email Communications	This filter selects events that indicate failed email communications.	Filter
Email Traffic	This filter selects events indicating successful email communications.	Filter
Windows Security Enabled Group Membership Change	This filter selects events indicating a Windows object was added to or removed from a security enabled group.	Filter
Unsuccessful Windows Logins for Valid Username	This filter identifies unsuccessful login events for a valid username recorded on Microsoft Windows domain controllers.	Filter
Role - DBA	This filter selects events attributable to actors having a role of dba.	Filter
Successful and Unsucessful Logins - Windows 2003	This filter identifies both successful and unsuccessful logins on Windows 2003 domain controller machines.	Filter
Employee Type - Part Time	This filter selects events involving users having an employee status type of Part Time.	Filter

Resource	Description	Type
After Hours	This filter defines the time period of after hours. Change this filter to adjust the default settings.	Filter
User Privilege Added or Revoked	This filter selects events indicating a specific privilege was added or revoked.	Filter
Non-ArcSight Internal	This filter excludes internal ArcSight events.	Filter
Failed Logins - Application	This filter selects events indicating login failures to applications.	Filter
Unsuccessful or Attempted Logins	This filter identifies all login events in which the outcome was not a definite success, in other words either a failure or an attempt.	Filter
All Database Activity	This filter selects all database activity.	Filter
All Failed Logins	This filter selects all events indicating that a user failed authentication.	Filter
User Expired from Pending Stale Accounts List	This filter selects events indicating that a user has expired from the Pending Stale Accounts active list, indicating the account has not been used in 6 months.	Filter
Successful Logins - Application	This filter selects events indicating successful logins to applications.	Filter
ASM Events	This filter selects internal monitoring events involving data monitor resources.	Filter
Successful Logins - Windows 2003	This filter identifies successful login events to Windows 2003 domain controller machines.	Filter
Successful Web Page Access	This filter identifies successful Web page access reported by proxy servers. Modify this filter to select events that match your environment if needed.	Filter
Unix Events	This filter selects events that are coming from Unix devices.	Filter
User Privilege Revoked	This filter selects events indicating that user rights were removed.	Filter
Successful Print Job	This filter shows successful print jobs.	Filter
Building Access Events	This filter selects all building access events, such as a user badging into a building.	Filter
Employee Type - Full Time	This filter selects events attributable to actors having an employee type of Full Time.	Filter
Database Authentication	This filter selects database authentication events.	Filter
Database Table Access	This filter looks at access patterns of tables in a database.	Filter
Successful Logins - Windows 2008	This filter identifies successful login events to Windows 2008 domain controller machines.	Filter
Address or Username Present	This filter checks whether any of attacker address, attacker username, or target username are present in the event.	Filter
Attacker and Target Username Not Equal	This filter selects events in which the attacker and target user names are both populated, and with differing values.	Filter

Resource	Description	Type
Failed Logins - Server	This filter selects events indicating login failures to servers.	Filter
Successful Logouts - Server	This filter selects events indicating successful server logouts.	Filter
User Group Membership Changes	This filter selects events indicating a user group membership change within an application.	Filter
Successful Building Access Events	This filter selects successful building access events.	Filter
Arcsight Internal Events	This filter selects ArcSight ESM internally generated events.	Filter
Successful Logins - Server - Actor NOT NULL	This filter selects events indicating successful logins to servers where the target user name can be correlated to an actor.	Filter
Proxy Event Categorization	This filter selects events indicating proxy traffic. The filter conditions are written considering the categorization of known proxy events.	Filter
Printing Activity	This filter selects events indicating printing activity.	Filter
Username Present	This filter checks whether any of attacker username, or target username are present in the event.	Filter
Successful Database Access	This filter selects events indicating successful access of databases.	Filter
All Printing Events	This filter selects events indicating printing activity.	Filter
Printing After Hours	This filter selects events that indicate printing activity occurring after hours.	Filter
Unsuccessful Logins for Valid Username - Windows 2008	This filter identifies unsuccessful logins for a valid username on Windows 2008 domain controller machines.	Filter
Target User Name is NULL	This filter selects events in which the target user name field is not populated.	Filter
Windows Events	This filter selects all events in which the device product field is Microsoft Windows.	Filter
Unsuccessful Logins for Valid Username - Windows 2003	This filter identifies unsuccessful logins for a valid username on Windows 2003 domain controller machines.	Filter
Logins - Failed - GeoCountry to User	Identifies patterns related to failed login by countries. By default, patterns will be identified when the same set of one or more accounts have failed logins from two or more different attacker countries and target IPs combinations.	Profile
Building Egress Events	This filter selects all building egress events, such as a user badging out of a building.	Filter
User Lookup on Dark Website	Identifies if a user's email address is available on the dark web.	Integration Command
Logins - Successful - User to IP Address	This pattern discovery profile identifies patterns in user login activity. By default, patterns will be identified when the same set of two or more target IP addresses are logged into by two or more different users.	Profile

Resource	Description	Type
URL Access - Time Based	This pattern discovery profile identifies patterns in URL browsing activity. By default, patterns will be identified when the same set of two or more URLs are visited by two or more different users. Snapshots generated by this profile will show the percentage of events that occur in the same sequence. The events processed by this profile must match the Proxy Traffic filter.	Profile
User Activity	This pattern discovery profile identifies patterns in user activity. By default, patterns will be identified when the same set of two or more events are seen from two or more different users.	Profile
Logins - Failed - Address to User	This pattern discovery profile identifies patterns in failed login activity. By default, patterns will be identified when the same set of two or more accounts have failed logins from two or more different machines.	Profile
User Activity - Differing Hosts	This pattern discovery profile identifies patterns in user activity. By default, patterns will be identified when the same users are seen communicating across two or more different attacker and target address pairs.	Profile
Logins - Successful - User to Application	This pattern discovery profile identifies patterns in successful application login activity. By default, patterns will be identified when the same set of two or more accounts have successful logins to two or more different applications.	Profile
Logins - Successful - User to Hostname	This pattern discovery profile identifies patterns in user login activity. By default, patterns will be identified when the same set of two or more target hostnames are successful logged into by two or more different users.	Profile
URL Access	This pattern discovery profile identifies patterns in URL browsing activity. By default, patterns will be identified when the same set of two or more URLs on a given server are visited by two or more different users. The events processed by this profile must match the Proxy Traffic filter.	Profile
User Activity - Differing Attacker and Target Usernames	This pattern discovery profile identifies patterns in user activity. By default, patterns will be identified when the same set of two or more events are seen from two or more groupings of differing attacker and target user names. This might happen, for example, when administrators make the same modifications to multiple user accounts. The events processed by this profile must have a username present.	Profile
All Activity for Known Actors	This query selects all events that can be attributed to any actor in the system.	Query
After Hours Building Accesses	This query selects events indicating after hours building access.	Query
Failed Server Logins for Employee Type	This query selects the actor's full name, device product, and count from events indicating a failed login to a server by an actor having the specified employee type.	Query
Top Blocked Actors by Account ID	This query selects the top actors by number of events that have requests blocked by proxy servers. The actors are derived by virtue of their account IDs.	Query
Physical Access Activity for Department	This query shows all the physical access activity for the specified department.	Query

Resource	Description	Type
Top Bandwidth - Download - by IP	This query selects the top actors that have the most number of bytes downloaded via proxy servers. The actors are derived by virtue of the event source IP address.	Query
Top Blocked Actors by IP (Size)	This query selects the top actors by data transferred that have requests blocked by proxy servers. The actors are derived by virtue of the event source IP address.	Query
Top Email Receivers (Amount)	This query selects the top email recipients based on the number of emails received.	Query
All Activity for Specific Actor - Details	This query selects information from events attributable to the specified actor.	Query
Building Access and Egress Totals - Trend	This query captures the total number of building access and egress events.	Query
Group Membership Changes	This query selects information from events indicating a user group membership change within an application.	Query
Printing Activity for Specific Actor	This query selects printing activity for the specified actor.	Query
Proxy Trend	This query selects information needed to capture aggregated proxy usage over the short term.	Query
Successful Application Logins for Employee Type	This query selects the actor's full name, device product, and count from events indicating a successful login to an application by an actor having the specified employee type.	Query
Top Blocked Actors by Account ID (Size)	This query selects the top actors by data transferred that have requests blocked by proxy servers. The actors are derived by virtue of their account IDs.	Query
Stale Accounts	This query retrieves a list of stale account IDs with the associated actor and device information.	Query
Top Actors Badging In	This query selects those actors that have the most number of successful building access events.	Query
Top Email Senders (Size)	This query selects the top email senders based on the size of emails sent.	Query
Top Accessed Websites (Size)	This query selects the top accessed web sites by data transferred.	Query
Top Blocked Websites	This query selects the top blocked websites by number of events.	Query
Successful Server Logins for Role	This query selects the actor's full name, device product, and count from events indicating a successful login to a server by an actor having the specified role.	Query
Failed Application Logins for Role	This query selects the actor's full name, device product, and count from events indicating a failed login to an application by an actor in the specified role.	Query
Top Bandwidth - Upload - by Account ID	This query selects the top actors that have the most number of bytes uploaded via proxy servers. The actors are derived by virtue of their account IDs.	Query
Failed Application Logins for Employee Type	This query selects the actor's full name, device product, and count from events indicating a failed login to an application by an actor having the specified employee type.	Query
UBM - Open Cases	This query selects the open UBM cases.	Query

Resource	Description	Type
Successful Application Logins for Department	This query selects the actor's full name, device product, and count from events indicating a successful login to an application by an actor in the specified department.	Query
All Activity for Role	This query selects the actor full name, vendor, product, event name, and count of all events that can be correlated to an actor having the specified role.	Query
Top Blocked Actors by IP	This query selects the top actors by number of events that have requests blocked by proxy servers. The actors are derived by virtue of the event source IP address.	Query
Successful Building Access Events Over the Past Day	This query selects successful building access events per hour over the past day.	Query
Building Egress Events Over the Past Week	This query captures the total number of building egress events per day over the past week.	Query
Privilege Added or Revoked for Department	This query selects information from events indicating a specific privilege was added or revoked. The search is limited to actors in the specified department.	Query
Successful Server Logins for Employee Type	This query selects the actor's full name, device product, and count from events indicating a successful login to a server by an actor having the specified employee type.	Query
All Activity for Employee Type	This query selects the actor full name, vendor, product, event name, and count of all events that can be correlated to an actor having the specified employee type.	Query
Top Largest Emails	This report shows the largest emails that have been sent.	Query
Websites Accessed by Actor - Month	This query selects all the websites visited by the specific actor over the past month.	Query
All Actions for Actor	This query gets aggregated information about events that might be attributable to actors.	Query
Top Blocked Web Pages (Size)	This query selects the top blocked web pages by data transferred.	Query
UBM - Top Rule Firings	This query selects the rules that trigger the most in the UBM solution.	Query
Printing Volume in Pages Review	This query selects printing volume in pages by user.	Query
Top Accessed Web Pages (Size)	This query selects the top accessed web pages by data transferred.	Query
Successful Server Logins for Department	This query selects the actor's full name, device product, and count from events indicating a successful login to a server by an actor in the specified department.	Query
SU and SUDO Activity	This query selects all activity related to su or sudo on UNIX machines. The attackerUser is trying to execute code with the privileges of the targetUser.	Query
Building Egress Events Over the Past Day	This query captures the total number of building egress events per hour over the past day.	Query
Physical Access Activity for Actor	This query shows all the physical access activity for the specified actor.	Query

Resource	Description	Type
Top Bandwidth - Download - by Account ID	This query selects the top actors that have the most number of bytes downloaded via proxy servers. The actors are derived by virtue of their account IDs.	Query
Top Email Receivers (Size)	This query selects the top email recipients based on the size of emails received.	Query
Top Accessed Web Pages	This query selects the top accessed web pages by number of events.	Query
All Activity for Specific Actor - Chart	This query selects the application and count of events attributable to the specified actor.	Query
Uncommon Websites	This query identifies those websites that were accessed by less than three actors by default. To change the default number of actors, modify the Group By conditions in the query.	Query
All Activity for Department - Chart	This query selects the application and count of all events that can be correlated to an actor belonging to the specified department.	Query
Top Email Senders (Amount)	This query selects the top email senders based on the number of emails sent.	Query
Actor by IP - Websites Accessed	This query selects websites accessed by actors who were derived from the base events by virtue of the event source IP address.	Query
Top Bandwidth - Upload - by IP	This query selects the top actors that have the most number of bytes uploaded via proxy servers. The actors are derived from by virtue of the event source IP address.	Query
Badged In Actor Details	This query shows relevant actor base attribute information for those actors that are currently badged in.	Query
Hourly Application Access Per User	This query selects the device product, hour, and count from events indicating a successful application login by the specified actor.	Query
Privilege Added or Revoked for Employee Type	This query selects information from events indicating a specific privilege was added or revoked. The search is limited to actors having the specified employee type.	Query
Privilege Added or Revoked	This query selects information from events indicating a specific privilege was added or revoked.	Query
Top Blocked Websites (Size)	This query selects the top blocked websites by data transferred.	Query
Actors by Account ID - Websites Accessed	This query identifies websites accessed by actors who were derived from the base events by virtue of their account IDs.	Query
Physical Access System Events	This report shows successful building access events.	Query
Activity Based Modeling by Employee Type	This query selects the vendor, product, and target asset network domain from events which can be correlated to an actor. The actor's employee type is also selected.	Query
Group Membership Changes for Department	This query selects information from events indicating a user group membership change within an application. The search is limited to actors within the specified department.	Query
Weekly Proxy Trend	This query selects information needed to capture aggregated proxy usage over a week.	Query

Resource	Description	Type
Activity Based Modeling by Department	This query selects the vendor, product, and target asset network domain from events which can be correlated to an actor. The actor's department is also selected.	Query
Pending Stale Accounts	This query retrieves a list of pending stale account IDs with the associated actor and device information.	Query
Top Badged In Locations	This query selects the top locations that have the most number of successful building access events.	Query
Websites Accessed by Actor - Day	This query selects all the websites visited by the specific actor over the past day.	Query
Failed Application Logins for Department	This query selects the actor's full name, device product, and count from events indicating a failed login to an application by an actor in the specified department.	Query
Failed Server Logins for Department	This query selects the actor's full name, device product, and count from events indicating a failed login to a server by an actor in the specified department.	Query
Top Departments with Badged In Actors	This query selects the top departments that have the most number of successful building access events.	Query
Average of Hourly Application Access	This query selects the actor's unique id, device product, hour, and count from events indicating a successful login by an actor having the specified role.	Query
Successful Application Logins for Role	This query selects the actor's full name, device product, and count from events indicating a successful login to an application by an actor having the specified role.	Query
All Activity for Department	This query selects the actor full name, vendor, product, event name, and count of all events that can be correlated to an actor belonging to the specified department.	Query
Activity Based Modeling by Role	This query selects the vendor, product, and target asset network domain from events which can be correlated to an actor. The actor's role is also selected.	Query
Top Proxy Users (Size)	This query selects the top users accessing websites by data transferred.	Query
Top Accessed Websites	This query selects the top accessed web sites by number of events.	Query
Top Roles with Badged In Actors	This query selects the top roles that have the most number of successful building access events. For a role to be selected at least two actors must have the same role.	Query
Successful Building Access Events Over the Past Week	This query selects successful building access events per day over the past week.	Query
Failed Server Logins for Role	This query selects the actor's full name, device product, and count from events indicating a failed login to a server by an actor having the specified employee type.	Query
Top Proxy Users	This query selects the top users accessing websites by number of events.	Query
Hourly Server Access Per User	This query selects the server name, hour, and count from events indicating a successful application login by the specified actor.	Query
UBM - Case Chart	This query selects cases per operational impact and stage.	Query

Resource	Description	Type
Top Countries with Badged In Actors	This query selects the top countries that have the most number of successful building access events.	Query
Top Blocked Web Pages	This query selects the top blocked web pages by number of events.	Query
Printing Volume in Bytes Review	This query selects printing volume in bytes by actor.	Query
Average of Hourly Server Access	This query selects the actor's unique id, device product, hour, and count from events indicating a successful login to a server by an actor having the specified role.	Query
All Activity for Employee Type - Chart	This query selects the application and count of all events that can be correlated to an actor having the specified employee type.	Query
Daily Active Accounts	This query retrieves a list of pending stale account IDs with the associated actor and device information.	Query
URLs Accessed	This query selects the accessed URLs and the number of times they were accessed.	Query
Total Number of Badged In Actors	This query selects the total number of currently badged in actors.	Query
All UBM Cases	This query selects all cases in the UBM case group.	Query
IP Address to Actor Map	This session list tracks the IP addresses that can be associated with actors. Typically, these IP addresses will belong to single-user machines.	Session List
Weekly Proxy Activity	This weekly trend collects information needed to capture aggregated proxy usage.	Trend
Proxy Activity	This hourly trend collects information needed to capture aggregated proxy usage.	Trend
Building Access and Egress	This hourly trend captures the total number of building access and egress events.	Trend
All Actions for Actor	This hourly trend collects aggregated information about events that might be attributable to actors.	Trend

Privileged User Monitoring Use Case

The Privileged User Monitoring use case monitors the usage and authorization of privileged accounts.

The resources provided in the Privileged User Monitoring use case enable auditors, analysts, and managers to provide the following services:

- Monitor and report when actors are added or removed from a privileged group
- Monitor and report when actors are added and then removed from a privileged group in a short amount of time
- Monitor and report on activity of privileged users by role, employee type, and department
- Monitor and report on failed or successful privileged user login events by actor, department, and role
- Monitor and report on the suspicious activity of privileged accounts

- Monitor and report on rule firings for privileged actors, departments and job titles
- Detect patterns of activity across privileged role additions and deletions
- Detect patterns of privileged user activity across actors
- Report on the suspicious activity and rule firings of privileged actors/users. These reports and query viewers are based on the Actor Changes and Actor Changes trends.

This use case determines that actors have been added or removed from a privileged group by processing events from the sources:
-Events from devices
-Internal events indicating a manual change to an actor using the ESM Console
-Internal events indicating a change to an actor by the Actor Model Import connector

Devices

The following devices can supply events to this use case:

- Operating System
- Intrusion Detection System/Intrusion Prevention System
- Application

All devices listed above can supply events to this use case but the resources will only process events from devices, when the device generates events that can be attributed to specific actors.

Configure Resources

Configure the following types of resources for this use case:

- Active Lists
- Rules
- Filters
- Trends and Queries

Active Lists

The following active lists should be configured for this use case:

- Configure the Privileged User Roles active list with privileged user groups used in your organization, such as Enterprise Admins and Domain Admins. Enter the group names exactly as specified in Active Directory. **This list should be maintained.**

- Optional—Configure the Time To Live (TTL) for the Actor Added to Privileged Group active list to a period of time that is considered suspicious for an account to be added and then quickly removed in your organization. For example, if it is suspicious for an account to be added and removed from a privileged group within 2 days, set the TTL value of the list to 2 days.

Rules

The following rules should be enabled for this use case:

Enable the Actor Added to Privileged Group rule for this use case. By default, this rule invokes the following action:

- **Set Event Field Actions**—Sets field values for the event generated by this rule.

By default, the following action of this rule is disabled. You can optionally enable this action:

- **Add to Existing Case**—If this action is enabled and the rule is triggered, the rule adds a case to the specified URI. For more information, see .

Enable the Monitor Actor Added to Privileged Group rule for this use case. By default this rule invokes the following actions:

- **Set Event Field Actions**—Sets field values for the event generated by this rule.
- **Add to Active List**—Add the UUID, Full Name, and Privileged Group to the Actor Changes active list.

Enable the Actor Removed From Privileged Group rule for this use case. By default, this rule invokes the following action:

- **Set Event Field Actions**—Sets field values for the event generated by this rule.

By default, the following action of this rule is disabled. You can optionally enable this action:

- **Add to Existing Case**—If this action is enabled and the rule is triggered, the rule adds a case to the specified URI. For more information, see .

The following rule can be enabled for this use case:

Enable the Actor Added and Removed From Privileged Group Within Short Time rule if you want to track when an actor has been added and then removed in a short amount of time. By default, this rule invokes the following actions:

- **Set Event Field Actions**—Sets field values for the event generated by this rule.
- **Remove from Active List**—Remove the entry for the actor from the Actor Changes active list.

By default, the following action of this rule is disabled. You can optionally enable this action:

- **Add to Existing Case**—If this action is enabled and the rule is triggered, the rule adds a case to the specified URI. For more information, see .

Filters

Verify that the following filters detect events in your environment when an account is added or removed from a group:

- Actor Added to Privileged Group
- Actor Removed from Privileged Group

Trends and Queries

Reports and query viewers in this use case are based on the following trends:

- Privileged User Actions— Enable this trend for this use case. This trend depends on the All Actions for Actor trend being enabled.
- Actor Changes— Enable this trend for this use case. This trend depends on the Threat Score Contributors trend being enabled.
- Threat Score Contributors for Privileged Users—This trend is included with the Actor Threat Score Use Case. Several resources in this use case require that this trend be enabled.

Before enabling the Threat Score Contributors trend, customize the following queries to reflect the privileged roles used in your environment:

- Threat Score Rule Firings for Privileged Users - Trend
- Threat Score Rule Firings for Non-Privileged Users

All Actions for Actor—This trend is included with the User Activity Monitoring Use Case. Several resources in this use case require that this trend be enabled. Before enabling the Actor Changes trend, customize the query to reflect the privileged roles used in your environment.

Before enabling these trends, verify that these trends collect the expected events for your environment. In addition, you might want to customize the trends before enabling.

Verify Configuration

Verify that actors with privileged roles are detected:

1. In the Navigator panel, go to **Dashboards**.
2. Navigate to `ArcSight Solutions/UBM/Privileged User Monitoring/`.
3. Right-click Privileged User Summary and select Show Dashboard.

Resources

The following table lists all the resources explicitly assigned to this use case and any dependent resources. Each resource can be accessed from the Privileged User Monitoring use case landing page: /All Use Cases/ArcSight Solutions/UBM/Actor Management, or their URI, for example: /All <Resource Type>/ArcSight Solutions/UBM/<Use Case>/<Resource Name>.

Resource	Description	Type
Monitor Resources		
Privileged User Summary	Displays important aspects of actors added to privileged groups.	Dashboard
Failed Privileged User Actions	This dashboard displays Failed Administrative Actions information.	Dashboard
Privileged User Summary	This dashboard shows some important aspects of actors added to privileged groups.	Dashboard
Unsuccessful Privileged User Logins	This dashboard displays information around failed privileged user logins.	Dashboard
Privileged User Activity	This query viewer displays the latest activity by privileged users.	Query Viewer
Actors with Privileged Roles	This query viewer shows actors with privileged roles and the total number of roles each such actor has.	Query Viewer
Threat Score Rule Firings for Non-Privileged Users	This query gets information about actor threat score correlation events for non-privileged users.	Query Viewer
Suspicious Activity by Privileged Users	This query viewer shows the latest information from all suspicious events that can be correlated to a privileged user.	Query Viewer
Non-Admins with Privileged Roles	This query viewer shows actors that have privileged roles but do not have Admin as part of their DN.	Query Viewer
Threat Score Rule Firings for Privileged Users	This query viewer gets information about actor threat score correlation events for privileged users.	Query Viewer
Successful Privileged User Logins for Role	This report shows a count of successful logins by privileged users with the specified roles.	Report
Actor Added to Privileged Group	This report shows actors who were added to privileged groups such as the Administrators group.	Report
Failed Privileged User Logins	This report shows a count of failed privileged user logins per actor.	Report
Actor Removed from Privileged Group	This report shows actors who were removed from privileged groups such as the Administrators group.	Report
Failed Privileged User Logins for Department	This report shows a count of failed logins by privileged users in the specified department.	Report

Resource	Description	Type
Actor Added and Removed from a Privileged Group in a Short Time	This report shows events indicating an actor was added and removed from a privileged group in a short period of time.	Report
Activity Summary for Privileged Actors	This report shows a count of the number of events for each privileged actor per product.	Report
All Privileged User Activity for Department	This report shows a summary of events that can be correlated to a privileged actor belonging to the specified department.	Report
All Privileged User Activity for Employee Type	This report shows a summary of events that can be correlated to a privileged actor having the specified employee type.	Report
Successful Privileged User Logins for Department	This report shows a count of successful logins by privileged users in the specified department.	Report
Activity Summary for Privileged Actors on the Threat Score List	This report shows a count of the number of events for each privileged actor that is on the threat score list per product.	Report
All Privileged User Activity for Role	This report shows a summary of events that can be attributed to a privileged user with a specified role.	Report
Successful Privileged User Logins for Actor Full Name	This report shows a count of successful logins for the specified privileged user.	Report
Failed Privileged User Logins for Role	This report shows a count of failed logins by privileged users with the specified roles.	Report
Library - Correlation Resources		
Actor Added to Privileged Group	This rule triggers when an actor is assigned a privileged role.	Rule
Monitor Actor Added to Privileged Group	This rule creates an entry in an active list when an actor is added to privileged group. The active list is used to track additions and removals of actors to privileged groups in a short time period.	Rule
Actor Added and Removed From Privileged Group Within a Short Time	This rule detects when actors are added and then removed from a privileged group in a short period of time.	Rule
Actor Removed From Privileged Group	This rule triggers when an actor is removed from a privileged role.	Rule
Library Resources		
Actor Added to Privileged Group	This active list stores actors who were added to a privileged group. It helps detects when this privilege is added and then removed within a short period of time.	Active List
Privileged User Roles	This active list is used to define user groups with elevated privileges.	Active List
Increase Actor Threat Score	This active list contains a list of suspicious activity rules and their customizable threat scores. When an actor causes one of these rules to trigger, their threat score is increased by the rule's threat score as defined in this list.	Active List

Resource	Description	Type
Account Authenticators	This active list is used by the actor global variables to determine what the Identity Management authenticator is, base on the event, so that an actor can be determined from event information.	Active List
Actor Threat Score	This list maintains a running threat score for actors exhibiting suspicious activity.	Active List
Network Domains	This is a solutions asset category.	Asset Category
Top 10 Privileged Users with Unsuccessful Logins	This data monitor displays privileged actor names with the most failed logins.	Data Monitor
Failed Privileged User Actions by Username Moving Average	This data monitor shows a moving average of failed actions by privileged users.	Data Monitor
Last 20 Actors Added to Privileged Groups	This data monitor shows the last 20 actors who were added to privileged groups.	Data Monitor
Failed Privileged User Actions by Device Moving Average	This data monitor shows a moving average of failed privileged user actions per device.	Data Monitor
Last 20 Failed Privileged User Action Events	This data monitor shows the last 20 failed privileged user actions.	Data Monitor
Actors Added and Removed from Privileged Group in a Short Time	This data monitor show the last time an actor was added and removed from a privileged group in a short period of time.	Data Monitor
Top 10 Privileged Users with Failed Actions	This data monitor shows the top 10 privileged users with failed actions in the last hour.	Data Monitor
Top 10 Network Domains with Unsuccessful Privileged User Logins	This data monitor provides an ordered list of the Network Domains with the most privileged user login failures.	Data Monitor
Top 10 Devices with Failed Privileged User Actions	This data monitor shows the top 10 devices products with failed actions by privileged users in the last hour.	Data Monitor
Last 20 Unsuccessful Privileged User Logins	This data monitor provides a list of the last 20 unsuccessful privileged user logins.	Data Monitor
Top 10 Hosts with Unsuccessful Privileged User Logins	This data monitor displays the hosts with most unsuccessful privileged user logins.	Data Monitor
ActorByAccountID	This global variable maps the account information in an event with an actor. The account information consists of the device vendor and product, and information derived from the attacker or target user name, with preference to the target user name.	Global Variable
ActorFromIPMap	This global variable returns an actor's UUID, full name, username used, and login type if the actor is associated with a source IP address.	Global Variable

Resource	Description	Type
ActorByAttackerUserName	This variable maps the account information in an event with an actor. The account information consists of the device vendor, device product, connector address, connector zone, and information derived from the attacker user name.	Global Variable
solnPatternDiscoveryConst	This variable returns a constant string that can be used in Pattern Discovery profiles when it is not required to specify either a Source or a Target event field.	Global Variable
ARST_IDV_ ActorUUIDByAuditOrBaseEvt	This global variable retrieves the Actor UUID from an audit, base, or correlation event.	Global Variable
ActorByTargetUserName	This variable maps the account information in an event with an actor. The account information consists of the device vendor, device product, connector address, connector zone, and information derived from the target user name.	Global Variable
ARST_IDV_DeletedRole	This global variable returns the deleted role from actor audit events.	Global Variable
ARST_IDV_ ActorFullNameByAuditOrBaseEvt	This global variable retrieves the actor Full Name from an audit, base or correlation event.	Global Variable
solnGetAuthenticator	This global variable extracts the authenticator from the event by looking up the Account Authenticators list using event fields.	Global Variable
solnGetUsername	This global variable returns user name in an event from target user name or attacker user name, with preference to the target user name.	Global Variable
ARST_IDV_getAuthenticator	This global variable gets the default authenticator for the event.	Global Variable
ARST_IDV_ActorFromAuditEvt	This global variable returns the modified Actor from actor audit events.	Global Variable
ARST_IDV_AddedRole	This global variable returns the added role from actor audit events.	Global Variable
ARST_IDV_ ActorByDeviceCustomString6	This global variable retrieves the actor using account information in deviceCustomString6. This can be useful for event Ids 632, 636 and 660 in Windows 2003.	Global Variable
Events with ActorByAccountID	This field set selects the fields appropriate for viewing events correlated with actor and can be customized for the UBM active channels.	Field Set
Actor Added and Removed from a Privileged Group in a Short Time	This filter identifies correlation events indicating an actor was added and removed from a privileged role within a short time.	Filter
Failed Privileged User Actions	This filter identifies failed actions by privileged users.	Filter
Target Username is a System Account	This filter selects events in which the target user name is a system account.	Filter
Successful Logins	This filter identifies successful logins by both administrative and non-administrative users across a variety of operating systems (Unix, Windows 2003, Windows 2008).	Filter

Resource	Description	Type
Member Removed from Privileged Group	This filter identifies events indicating a user was removed from a privileged group as defined by the Privileged User Roles active list.	Filter
Member Added to Privileged Group - Windows	This filter selects events indicating a Windows object was added to a privileged group. Privileged groups are defined in the Privileged User Groups active list.	Filter
ActorByAttackerUserName is NULL	This filter selects events which cannot be attributed to an actor based on the attacker user name field.	Filter
Login Attempts	This filter selects any attempts at logging into systems. It excludes machine logins into Microsoft Windows systems.	Filter
All Failed Logins	This filter selects all events indicating that a user failed authentication.	Filter
Actor Removed from Privileged Group	This filter identifies actors who were removed from a privileged role.	Filter
Attacker User Is Privileged User	This filter checks whether the attacker user is an administrator.	Filter
Attacker User Name is a System Account	This filter selects events in which the attacker user name is a system account.	Filter
Suspicious Activity	This filter selects events indicating suspicious activity that merits investigation.	Filter
Member Removed from Privileged Group - Windows 2008	This filter identifies Windows 2008 events that indicate a user is removed from a domain local, global or universal security group. These groups are defined in the Privileged User Roles active list.	Filter
Member Removed from Privileged Group - Windows	This filter selects events indicating a Windows object was removed from a privileged group. Privileged groups are defined in the Privileged User Groups active list.	Filter
Windows 2008 Authentication Ticket Request	This filter identifies Microsoft Windows 2008 events which indicate that a Kerberos authentication ticket was requested.	Filter
Attacker User Name is NOT NULL	This filter selects events in which the attacker user name field is populated.	Filter
Actor from Audit Event is NOT NULL	This filter checks if an actor can be retrieved from an actor audit event.	Filter
Privileged Role Added (Audit Event)	This filter identifies when a privileged role is added to an actor, based on the actor audit event.	Filter
Unsuccessful Privileged User Login	This filter identifies events that indicate unsuccessful logins by a privileged user.	Filter
Actor Audit Events - Role Changes	This filter selects actor audit events generated by ESM when an actor resource's role attribute is updated.	Filter
Actor Added to Privileged Group	This filter identifies actors who were given a privileged role.	Filter
Windows 2003 Authentication Ticket Request	This filter identifies Microsoft Windows Kerberos Authentication Ticket Request events. These events are generated when a user logs into an Active Directory domain.	Filter

Resource	Description	Type
Privileged Actor Activity Excluding Common Events	This filter selects events, that are not common such as login events and can be attributable to actors having a privileged role such as administrator or dba. This filter is primarily used in pattern discovery profiles to find patterns of uncommon activity across privileged users. Modify this filter as needed to exclude other common events.	Filter
Member Added to Privileged Group - Windows 2003	This filter identifies Windows 2003 events that indicate a user has added to a domain local, global or universal security group. These groups are defined in the Privileged User Roles active list.	Filter
Windows Events with a Non-Machine User	This filters identified Microsoft Windows events that have a non machine/system user either in the attacker or the target fields.	Filter
Member Removed from Privileged Group - Windows 2003	This filter identifies Windows 2003 events that indicate a user is removed from a domain local, global or universal security group. These groups are defined in the Privileged User Roles active list.	Filter
Privileged Actor Activity	This filter selects events attributable to actors having a privileged role such as administrator or dba.	Filter
Unsuccessful Logins	This filter identifies failed logins attempts.	Filter
Target User Name is NOT NULL	This filter selects events in which the attacker user name field is populated.	Filter
Login Attempts	This filter selects any attempts at logging into systems. It excludes machine logins into Microsoft Windows systems.	Filter
Successful Logins - Unix	This filter identifies successful login attempts to Unix machines.	Filter
Actor Audit Events - Role Added	This filter selects actor audit events generated by ESM when an actor resource's role attribute is added.	Filter
Windows Events with a Non-Machine User	This filters identified Microsoft Windows events that have a non machine/system user either in the attacker or the target fields.	Filter
Actor Audit Events - Role Deleted	This filter selects actor audit events generated by ESM when an actor resource's role attribute is deleted.	Filter
ActorByAttackerUserName is NOT NULL	This filter selects events in which the attacker user name field is populated, and the event can be attributed to an actor based on that field.	Filter
Threat Score Contributors	This filter selects rule trigger events that contribute to the Actor Threat Score.	Filter
Privileged Role Removed (Audit Event)	This filter identifies when a privileged role is removed from an actor, based on the actor audit event.	Filter
Target User Name is NULL	This filter selects events in which the target user name field is not populated.	Filter
Member Added to Privileged Group - Windows 2008	This filter identifies Windows 2008 events that indicate a user is added to a domain local, global or universal security group. These groups are defined in the Privileged User Roles active list.	Filter
Windows Events	This filter selects all events in which the device product field is Microsoft Windows.	Filter

Resource	Description	Type
Actor Audit Events	This filter selects all actor audit events generated by ESM when an actor resource is updated.	Filter
Member Added to Privileged Group	This filter identifies when a user is added to a privileged group as defined in the Privileged User Roles active list.	Filter
Privileged Role Additions	This profile can be used to detect patterns of privileged role additions.	Profile
Privileged Role Deletions	This profile can be used to detect patterns of privileged role deletions.	Profile
Privileged User Activity - Title	This pattern discovery profile identifies patterns in the activity of privileged users across job title. By default, patterns will be identified when the same set of two or more events are seen across two or more different privileged job titles. The events processed by this profile must have a username present that can be attributed to an actor that belongs to privileged groups.	Profile
Privileged User Activity	This pattern discovery profile identifies patterns in the activity of privileged users. By default, patterns will be identified when the same set of two or more events are seen from two or more different privileged actors. The events processed by this profile must have a username present that can be attributed to an actor that belongs to privileged groups.	Profile
Successful Privileged User Logins for Role	This query selects events indicating successful logins by a privileged user with a particular role.	Query
All Activity for Privileged Employee Type	This query gets a summary of events that can be correlated to a privileged actor having the specified employee type.	Query
Actor Added and Removed from a Privileged Group in a Short Time	This query selects correlation events that indicate an actor was added and removed from a privileged group within a short period of time.	Query
Successful Privileged User Logins for Full Name	This query selects events indicating successful logins by a privileged user with a particular full name.	Query
Actor Added to Privileged Group	This query retrieves actors who were added to privileged groups, indicating they were given a privileged role.	Query
All Privileged User Activity for Role	This query gets a summary of events that can be correlated to an actor having the specified role.	Query
Actor Removed from Privileged Group	This query retrieves actors who were removed from privileged groups, indicating they were removed from a privileged role.	Query
All Activity for Privileged Employee Type - Chart	This query selects the application and count of all events that can be correlated to a privileged actor having the specified employee type.	Query
Non Admins with Privileged Roles - Summary	This query selects actors that have privileged roles but do not have Admin as part of their DN.	Query
Actions for Privileged Users - Trend	This query selects all actions that can be attributable to privileged users.	Query

Resource	Description	Type
Privileged User Activity	This query displays the latest events that include a privileged user.	Query
Actors with Privileged Roles - Summary	This query queries actors with privileged roles and shows the total number of roles each such actor has.	Query
Threat Score Contributors - Trend	This query gets aggregated information about correlation events for rules that contribute to an actor's threat score.	Query
Failed Privileged User Logins for Role	This query selects events indicating a failed login by a privileged user with a particular role.	Query
All Privileged Activity for Department - Chart	This query selects the application and count of all events that can be correlated to a privileged user belonging to the specified department.	Query
Suspicious Activity by Privileged Users	This query selects the latest information from all suspicious events that can be attributed to a privileged user.	Query
Threat Score Rule Firings for Privileged Users	This query gets information about actor threat score correlation events for privileged users.	Query
Failed Privileged User Logins	This query selects events indicating a failed login by a privileged user.	Query
Activity Summary for Privileged Actors on the Threat Score List	This query counts the number of events for each privileged actor on the threat score list per product.	Query
Threat Score Rule Firings for Non-Privileged Users	This query gets information about actor threat score correlation events for non-privileged users.	Query
All Actions for Actor	This query gets aggregated information about events that might be attributable to actors.	Query
All Privileged Activity for Department	This query gets a summary of events that can be correlated to a privileged actor belonging to the specified department.	Query
Successful Privileged User Logins for Department	This query selects events indicating a successful login by a privileged user in a particular department.	Query
Failed Privileged User Logins for Department	This query selects events indicating a failed login by a privileged user in a particular department.	Query
Threat Score Rule Firings for Privileged Users - Trend	This query gets information about actor threat score correlation events for privileged users.	Query
Activity Summary for Privileged Actors	This query counts the number of events for each privileged actor per product.	Query
IP Address to Actor Map	This session list tracks the IP addresses that can be associated with actors. Typically, these IP addresses will belong to single-user machines.	Session List
Privileged User Actions	This hourly trend collects aggregated information about events that might be attributable to privileged users.	Trend

Resource	Description	Type
Threat Score Contributors for Privileged Users	This trend captures a summary of all the rules that triggered and contribute to the threat scores of privileged users.	Trend
All Actions for Actor	This hourly trend collects aggregated information about events that might be attributable to actors.	Trend
Threat Score Contributors	This trend captures a summary of all rules that trigger and contribute to the threat scores of actors.	Trend

Federation Services Use Case

Federation Services is a use case that provides resources for Active Directory Federation Services (AD FS). AD FS helps ensure secure single sign-ons across organizations, so monitoring these logs is essential for maintaining the health and security of your environment. These resources, listed in the table below, enhance your ability to extract valuable insights from your AD FS logs and protect your single sign-on environments.

Federation Services requires the ArcSight SmartConnector for Windows Event Log - Native. You must configure this SmartConnector to collect events from the host's Active Directory.

Resources

The following table lists all the resources explicitly assigned to this use case and any dependent resources. Each resource can be accessed from the Federation Services use case landing page: /All Use Cases/ArcSight Solutions/UBM/Actor Management, or their URI, for example: /All <Resource Type>/ArcSight Solutions/UBM/<Use Case>/<Resource Name>.

Resource	Description	Type
Monitor Resources		
Monitor Successful MFA Token Validation	Displays successful MFA token validation events.	Active Channel
ADFS Health Check Status	Displays the top AD FS Health error and failure events. Before running this dashboard, ensure the following data monitors are enabled: • AD FS Health • AD FS Health Check Events - Bar Chart	Dashboard
Library - Correlation Resources		

Resource	Description	Type
Multiple Password Change Attempts Failed T1110.002	Detects when a user fails multiple password change attempts in a short time.	Rule
Extranet Lockout Event has Occurred T1110	Detects extranet lockout events. Extranet Lockout is a security feature that enables AD FS to stop authenticating malicious user accounts from outside the organization's network (extranet) for a specific period of time. This prevents the account from being locked out of the Active Directory, striking a balance between security and productivity.	Rule
Multiple Token Validations Failed by User in a Short Time T1078.002	Detects when a token validation fails multiple times from the same user.	Rule
Error During Token Validation T1087.002	Detects errors that occur during token validations.	Rule
Library Resources		
ADFS Health Check	Shows the top AD FS Health error and failure events.	Data Monitor
ADFS Health Check Events - Bar Chart	Shows the top AD FS Health error and failure events on bar chart format.	Data Monitor
Monitor Successful MFA Token Validation	Contains fields to monitor successful MFA token validation events.	Field Set
Successful MFA Token Validation	Captures events when an MFA token is successfully validated.	Filter
ADFS Health Errors and Failures	Filters for AD FS error or failure events.	Filter

Appendix A: Back Up and Uninstall IdentityView

IdentityView has been renamed to ArcSight User Behavior Monitoring (UBM). This section explains how to back up and uninstall IdentityView so that you can install the UBM package.

Note: Trend data cannot be preserved during the upgrade process.

Identify and Copy Customized Resources

(Optional) you can identify customized IdentityView 2.*n* resources by generating a list of resources that have changed since the solution packages were last exported. You can then copy those resources and use them as a reference for applying the same customizations to the UBM resources.

Note: Every time a package is exported, the change history is reset.

1. Log into the ESM Console as the ArcSight administrator.
2. In the Packages tab of the Navigator panel, expand the ArcSight Solutions group.
3. Right-click the IdentityView 2.0*n* solution package ( ) and select **Compare Archive with Current Package Contents.**

In the Viewer panel, a list of resources associated with the package is displayed. In the Change Since Archive column, any changes to the resource since the last export are displayed, either as Added, Modified, or Removed.

To sort the list and display the changed resources together, click the Change Since Archive column.

4. Optional: Copy and paste the cells from this table into a spreadsheet.
5. Copy the resources identified above by dragging them to a group outside of the IdentityView group hierarchy. For example, you might copy customized rules to Admin's Rules.
6. Use the copied resources as a reference to customize the UBM resources.

Copying the resources might cause dependency conflict errors, but after you install UBM, you can resolve the conflicts by right-clicking the resources and selecting Validate.

Back Up the IdentityView Active Lists and Session Lists

(Optional when upgradeing from IdentityView to UBM) Use the following procedure to back up the data in your IdentityView active lists and session lists, so you can import the data into UBM.

1. Log into the ESM Console.
2. In the Navigator panel, on the Packages tab, right-click Shared/All Packages/Public and select **New Package**.

The Package Editor opens in the Inspect/Edit panel.

3. On the Attributes tab, in the **Name** field, type a name for the package, for example, IdentityViewBackup, and make sure the **Format** field is set to default
4. On the Resources tab, click **Add**, then select **Lists|Active Lists**.
5. Check the box next to Active Lists/Shared/All Active Lists/ArcSight Solutions/IdentityView 2.n and click **OK**.

Alternatively, you can expand the IdentityView 2.n group and select individual lists.

6. On the Resources tab, click **Add** again, then select **Lists|Session Lists.**
7. Check the box next to Session Lists/Shared/All Session Lists/ArcSight Solutions/IdentityView 2.n and click **OK**.

Alternatively, you can expand the IdenityView 2.ngroup and select individual lists.

8. Check the **Children Only** boxes. Otherwise, when you import the backup package later, the IdentityView group name will revert to IdentityView 2.n rather than UBM 2.8.
9. Click **OK** to save the package.
10. In the Navigator panel, on the Packages tab, expand the Public folder, right-click the newly created backup package, select **Export Package to Bundle**, and save the .arb file to the local disk.
11. Right-click the backup package and select **Uninstall Package.**

Uninstall IdentityView

Use the following procedure to uninstall the IdentityView package.

1. In the Packages tab of the Navigator panel, expand the ArcSight Solutions group.
2. Right-click the IdentityView 2.*n* package ( ) and select **Uninstall Package**.
3. In the Uninstall Packages dialog, click **OK**.
4. In the Resolution Options window, choose **Skip** and then **Continue without saving changes**.
5. When the uninstall is finished, click **OK**.

Import the Backup Active Lists and Session Lists

Skip this section if you chose not to back up the active lists and session lists from the previous version of IdentityView.

1. On the new UBM package, import and install the backup .arb file that you created in to restore the data from the old active lists and session lists to the new lists.
2. After successfully importing the backup .arb file, right-click the active lists and session lists in the Navigator panel Resources tab and select **Show Entries** to display the restored entries.

Publication Status

Released: July 2024

Updated: Friday, September 27, 2024

Contact Information

We want to hear your comments and suggestions about this book and the other documentation included with this product. You can use the comment on this topic link at the bottom of each page of the online documentation, or send an email to MFI-Documentation-Feedback@opentext.com.

For specific product issues, contact OpenText Customer Care.

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 computer, click the link above and an email window opens with the following information in the subject line:

Feedback on Solutions Guide (User Behavior Monitoring 24.3)

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 MFI-Documentation-Feedback@opentext.com.

We appreciate your feedback!