Hewlett Packard
Enterprise

HPE Security ArcSight ESM: Brute Force Attack

Software Version: 1.0

Security Use Case Guide

March 31, 2017

Legal Notices

Warranty

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

The information contained herein is subject to change without notice.

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

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

This document is confidential.

Restricted Rights Legend

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

Copyright Notice

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

Support

Contact Information

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

Contents

Chapter 1: Overview

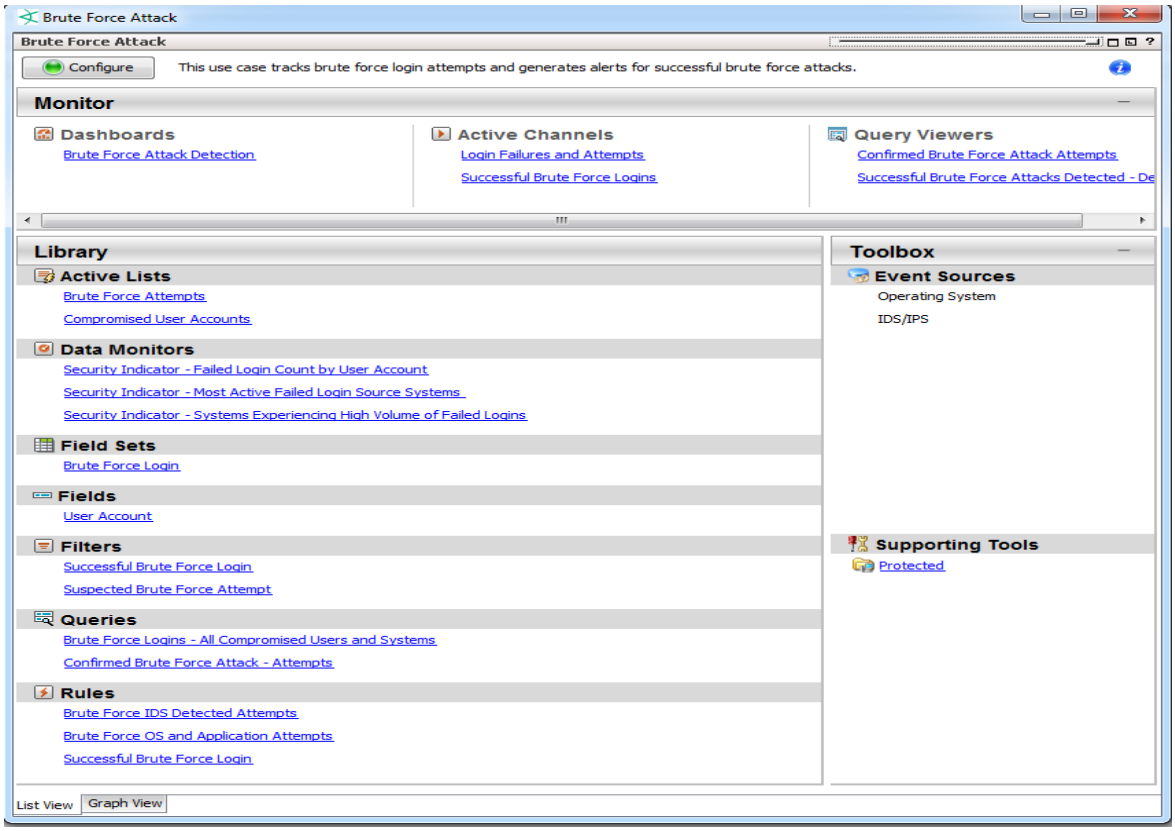
Brute force attacks apply trial-and-error methods to hack into a system and obtain encrypted information like passwords, personal identification numbers (PINs), and so on. A brute force program generates massive, consecutive log- in attempts.

The HPE ArcSight Brute Force Attack use case helps you identify brute force attempts and successful attacks on systems and applications, so you can protect your assets and user accounts from such attacks.

The use case tracks these brute force attacks in two phases.

- **First phase, track unsuccessful brute force attack attempts.** In the first phase, the use case tracks unsuccessful attacks in the form of
  - Unsuccessful brute force attempts on OS and applications. A rule looks for brute force attacks on OSs and applications. The rule triggers when the failed authentication event from the same attacker system using the same user account to the same target system exceeds the threshold. On first threshold, information about user account, attacker system and target system is added to an active list called **Brute Force Attempts**.
  - Unsuccessful attempts reported by the intrusion detection system (IDS). On the *first* attempt, the event information containing the user account, attacker system and target system is also added to the same active list.
- **Second phase, track successful brute force attacks:** The information is built from information collected by the rule on unsuccessful brute force attacks (first phase). If one successful login (attacker system, user account, target system) matches an entry in the Brute Force Attempts list, then this successful login event is considered a successful brute force attack. When a successful brute force attack is detected, information on the user account, attacker system, and target system is added to an active list called **Compromised User Accounts**.

The Brute Force Attack use case contains the following resources:



- A **dashboard** is provided to show an overview of successful and unsuccessful brute force login attempts. You can also view the security indicators used to classify the brute force login types being monitored. Through these security indicators, you can pinpoint probable brute force attacks against protected assets.
- Two **active channels**: The first channel enables you to investigate login failures and attempts; and the second channel enables you to investigate successful brute force logins. The active channels monitor login attempts from IDS (intrusion detection systems) and applications, respectively.
- Two **query viewers**: The first query viewer provides information on brute force attack attempts, and the second query viewer provides information on successful brute force attacks. Both query viewers are also available on the dashboard.

You can access the Brute Force Attack use case from the **Use Cases** tab of the ArcSight Console Navigator panel. The Monitor section of the use case lists the dashboard, active channels, and query viewers used to monitor and investigate brute force activity. The Library section of the use case lists all supporting resources that help collect information that goes on the dashboards and active channels.

The use case also provides a configuration wizard that guides you through required configuration.

This document describes how to install, configure, and use the Brute Force Attack use case and is designed for security professionals who have a basic understanding of ArcSightESM and are familiar with the ArcSight Console. For detailed information about using ArcSightESM, see the ArcSightESM

help system from the ArcSight Console**Help** menu. Find PDFs of all ArcSight documentation on Protect 724.

Chapter 2: Installation

To install the Brute Force Attack use case, perform the following tasks in the following sequence:

1. Download the Brute Force Attack use case zip file into the ArcSight Console system where you plan to install the use case, then extract the zip file.

   The zip file includes the *Brute_Force_Attack_1.0.arb* package, the accompanying Readme file, and the *Downloads_Groups_1.0.arb* package.
2. Log into the ArcSight Console as administrator.

   Note: During the package installation process, do not use the same administrator account to start another Console or Command Center session simultaneously. This login is locked until the package installation is completed.
3. Verify if you have a previous version of the use case package you want to install. If so, uninstall and delete this previous version:
   a. On the **Packages** tab of the Navigator panel, right-click the package and select **Uninstall Package**. The package icon is gray when it is uninstalled.
   b. Right-click the package and select **Delete Package**.
4. On the Packages tab, verify if **Downloads Groups** is already installed. If you see packages in `/All Packages/Downloads/Downloads Groups`, then ignore this step.

   If the Downloads Groups package is not present, import and install the *Downloads_Groups_1.0.arb* package. See "Importing and Installing a Package" on the next page for details.
5. Import and install the **Brute Force Attack** use case package. See "Importing and Installing a Package" on the next page for details.
6. Assign user permissions to the Brute Force Attack resources. See "Assigning User Permissions" on page 11 for details.

No configuration is required for the Brute Force Attack use case. However, before using the Brute Force Attack use case, make sure that you have populated your ESM network and asset models. A network model keeps track of the network nodes participating in the event traffic. Assets provide more granular attributes of the nodes, such as descriptions of critical servers. For information about populating the network model, refer to the *ArcSight Console User's Guide*.

Importing and Installing a Package

Follow the steps below to import and install the package(s). This assumes you have downloaded the zip file and extracted the contents into the ArcSight Console system.

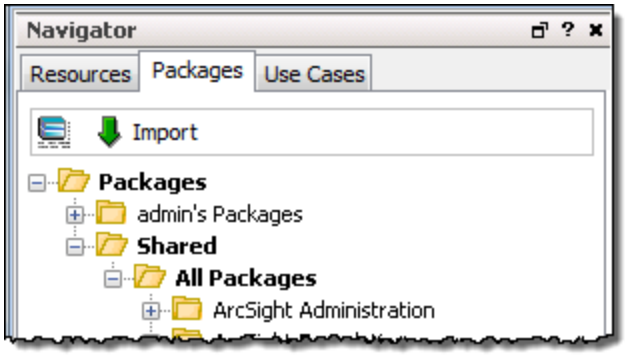
- If the ArcSight Console does not have the Downloads Groups package in `/All Packages/Downloads/Downloads Groups`, import and install the package first. Then repeat the steps to import and install the **Brute Force Attack** use case package.

  Note: The Downloads Groups package contains the groups used by the resources in the security use case; you must import and install this package first.

- If the Downloads Groups package is already installed, follow the steps to import and install the Brute Force Attack use case package only.

To import and install a package:

1. Log into the ArcSight Console as administrator. In the Navigator panel, click the **Packages** tab.



2. Click **Import**.
3. In the Open dialog, browse and select the package file (`*.arb`) you want to import, then click **Open**.
   The Importing Packages dialog shows how the package import is being verified for any resource conflicts.
4. In the Packages for Installation dialog, make sure that the check box is selected next to the name of the package you want to install and click **Next**.
   The Progress tab shows how the installation is progressing. When the installation is complete, the Results tab displays the summary report.
5. In the Installing Packages dialog, click **OK**. In the Importing Packages dialog, click **OK**.
6. On the **Packages** tab of the Navigator panel, expand the package group in `/All Packages/Downloads/` to verify that the package group is populated and that installation is successful.

Assigning User Permissions

By default, users in the `Administrators` and `Default User Groups/Analyzer Administrators` user groups can view and edit the resources. Users in the `Default User Groups` (and any custom user group under this group) can only view Brute Force Attack resources. Depending on how you set up user access controls within your organization, you might need to adjust those controls to make sure the resources are accessible to the right users.

Note: By default, the `Default User Groups/Analyzer Administrators` user group does not have edit permissions for archived reports in the Downloads group.

The following procedure assumes that you have logged into the ArcSight Console as administrator, and that you have set up the required user groups with the right users.

To assign user permissions:

1. In the Navigator panel, open the **Resources** tab.
2. For each of the resource types provided in the use case, navigate to `Downloads/Brute Force Attack`.
3. Right-click the `Brute Force Attack` group and select **Edit Access Control** to open the ACL editor in the Inspect/Edit panel.
4. Select the user groups for which you want to grant permissions and click **OK**.

Chapter 3: Configuration

Before configuring the use case, make sure that you have populated your ESM network model. A network model keeps track of the network nodes participating in the event traffic. For information about populating the network model, refer to the *ArcSight Console User's Guide*.

The Brute Force Attack use case requires the following configuration for your environment:

- Install the appropriate ArcSight SmartConnectors to receive relevant events from your intrusion device systems. For example, to receive relevant events from Cisco IOS IPS sensor devices, install the ArcSight SmartConnector for Cisco Secure IPS SDEE.
- Manually categorize all internal assets (assets inside the company network), or the zones to which the assets belong, with the **Protected** asset category (located in `/All Asset Categories/Site Asset Categories/Address Spaces/Protected`). Assets that are not categorized as internal to the network are considered to be external. Make sure that you also categorize assets that have public addresses but are controlled by the organization (such as Web servers) as **Protected**.

A configuration wizard is provided to guide you through some of the required configuration. Follow the procedure below.

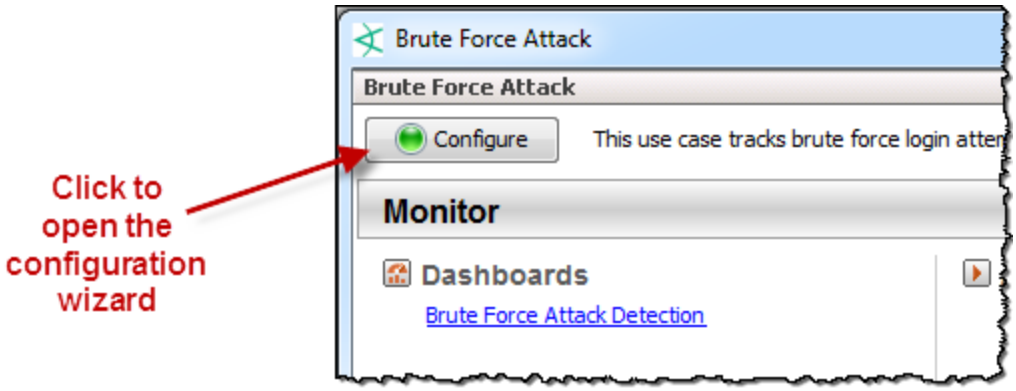
Note: You must categorize assets internal to the network manually; the procedure is not part of the configuration wizard. For information about categorizing assets, see the *ArcSight Console User's Guide*.

To configure the Brute Force Attack use case:

1. In the Navigator panel, click the **Use Cases** tab.
2. Go to the **Brute Force Attack** use case located in `/All Use Cases/Downloads/Hostile Activity Detection`.
3. Open the Brute Force Attack use case: either double-click the use case, or right-click the use case and select **Open Use Case**.

   The Brute Force Attack use case lists all the resources used for monitoring brute force activity.

4. Click the **Configure** button to open the configuration wizard.



5. Click **Next** to follow the configuration steps.

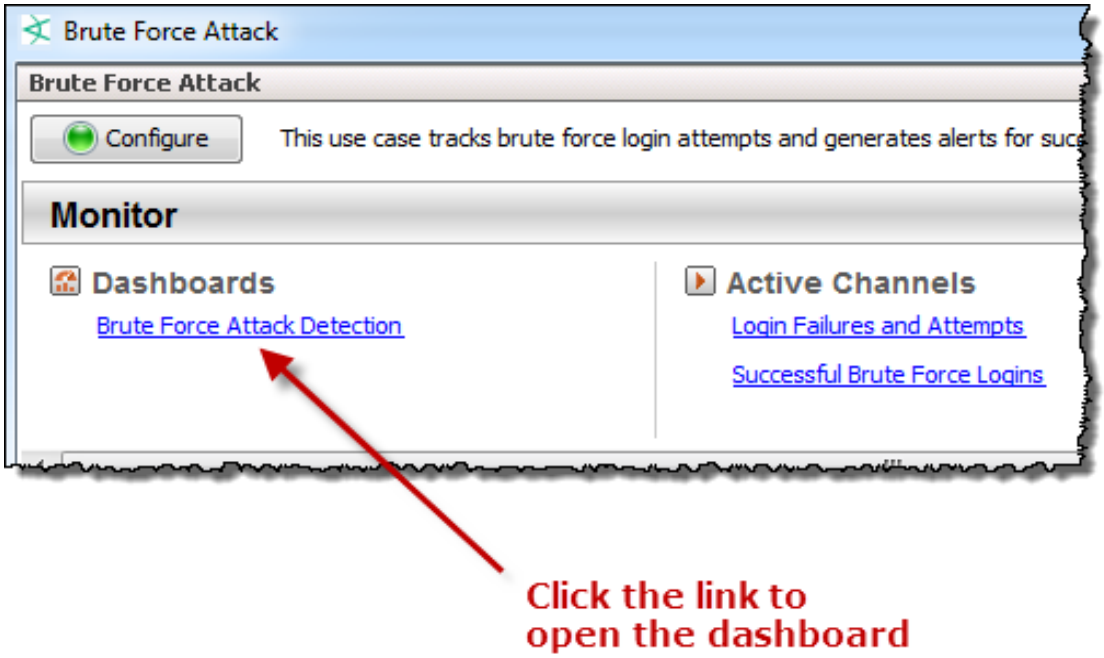
After you configure the Brute Force Attack use case, you are ready to monitor brute force activity. See "Getting Started with the Brute Force Attack Detection Dashboard" on page 15.

Chapter 4: Getting Started with the Brute Force Attack Detection Dashboard

The Brute Force Attack use case provides a dashboard to help you detect successful and failed attempts of a brute force attack.

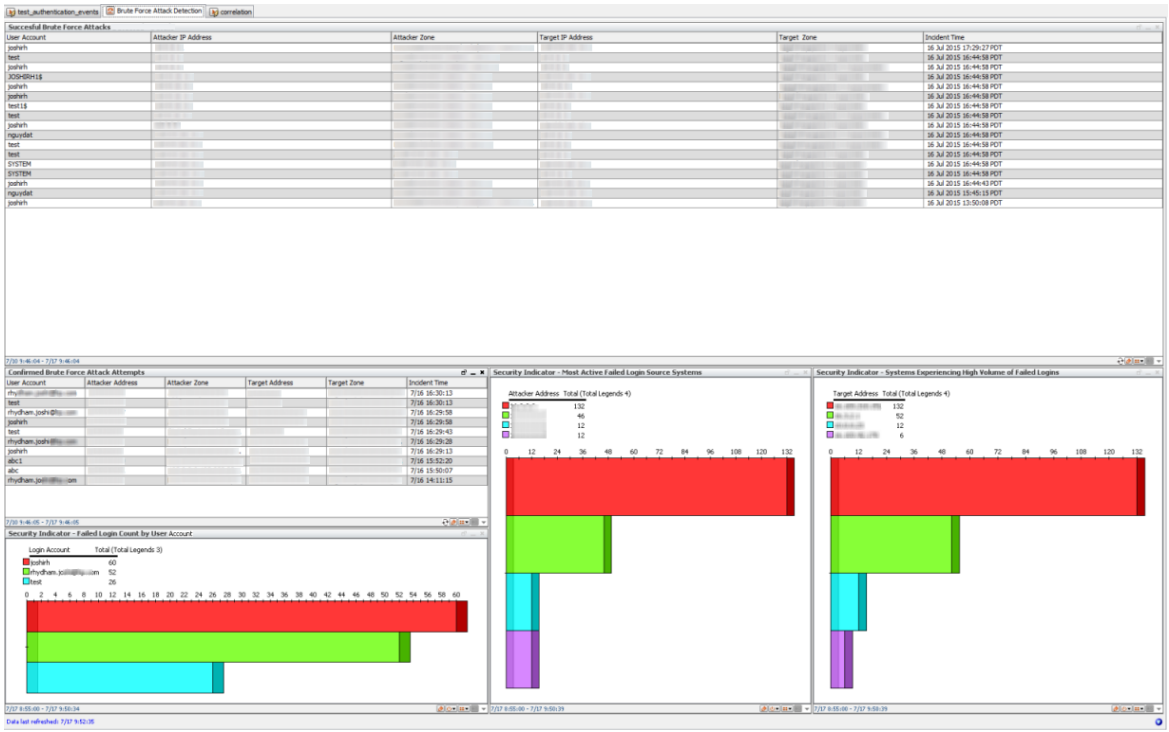
Use this dashboard to monitor confirmed brute force attacks and also monitor security indicators of failed logins: systems with high volumes of login failures, user accounts with failed logins, and source systems with the most failed logins.

To open the dashboard, click the link for the dashboard in the Brute Force Attack use case.



The dashboard opens in the Viewer panel of the ArcSight Console.

An example of the dashboard is shown below.



The following sections describe the data monitor and query viewer elements on this dashboard.

Data Monitors

The Brute Force Attack Detection dashboard includes three data monitors, security indicators of brute force attack attempts.

- **Security Indicator - Failed Logins Count by User Account**
  Refer to "Monitoring Failed Login Attempts" on page 19 for details about this data monitor.
- **Security Indicator - Most Active Failed Login Source Systems**
  Refer to "Monitoring Failed Logins from Attacker Systems" on page 24 for details on this data monitor.
- **Security Indicator - Systems Experiencing High Volume of Failed Logins**
  Refer to "Monitoring Failed Logins to Target Systems" on page 26 for details about this data monitor.

Query Viewers

Tip: Links to these query viewers are also available from the Brute Force Attack Use Case.

The Brute Force Attack Detection dashboard includes query viewers.

- **Confirmed Brute Force Attack Attempts**

  Refer to "Using the Confirmed Brute Force Attack Attempts Query Viewer" on page 23 for details about this query viewer.
- **Successful Brute Force Attack Attacks**

  Refer to "Using the Successful Brute Force Attacks Query Viewer" on page 32 for details about this query viewer.

Chapter 5: Monitoring Brute Force Attack Attempts

This chapter describes how you, the security analyst, can use the Brute Force Attack use case to identify brute force attempts against protected network assets and applications so that you can prevent future attempts.

Massive failed attempts constitute failed logins from the same attacker address using the same user account and targeting the same target system. By default, ten such failures within a minute is considered a brute force attack attempt.

The following topics are covered:

Monitoring Failed Login Attempts

User accounts used in attempted brute force attacks have the potential to be compromised, and you must ensure these accounts are investigated to prevent unauthorized use.

Watching Out for False Positives on Login Failures

When investigating failed login attempts, consider the following factors that can lead to false positives:

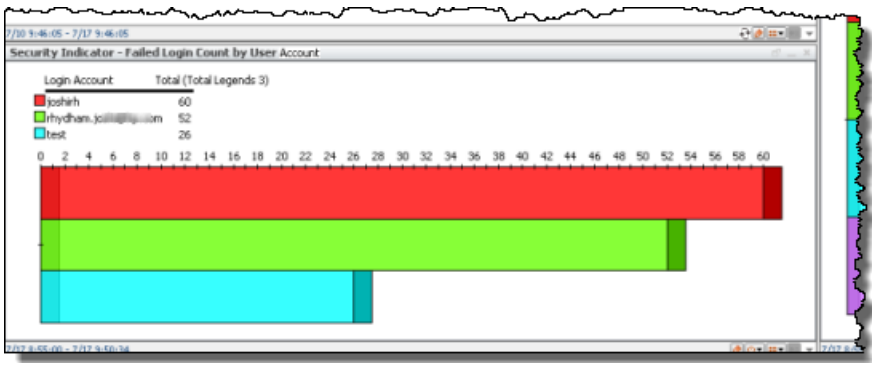
- The login attempt may come from a legitimate user logging in with an expired password. Expect a spike of such events if your business enforces a regular schedule of expiring passwords, requiring users to change their passwords. After a recent change, users are expected to use old passwords as a habit, until they are used to their new ones. After a brief period of adjustment, the failures should be reduced.
- Logins from applications and scripts may be using old and outdated configurations.

Take the necessary actions, for example, investigate further the failed user logins and update applications and scripts as required. After eliminating those legitimate login failures, you can focus on the failures that come from potential brute force attacks. For example, investigate if there is a business case for the user to access the target system.

Using the *Security Indicator - Failed Login Count by User Account* Data Monitor

This data monitor tracks, in real time, the user accounts that are sent in failed authentication events. Such failed authentications can be regarded as potential brute force attacks. The data monitor displays the number of times a user account was used in failed logins in five-minute buckets over an hour. The display refreshes every 30 seconds. Use this data monitor to track the user accounts associated with failed login events.

Below is a closeup of the data monitor:



To view the data monitor:

- On the Brute Force Attack use case's Dashboards section, click the link to the dashboard, **Brute Force Attack Detection**.

  Or

- On the ArcSight Console's resource Navigator panel:
  a. Go to `/All Dashboards/Downloads/Hostile Activity Detection`.
  b. Right-click Brute **Force Attack Detection** and select **Show Dashboard**.

The *Security Indicator - Failed Login Accounts Count by User Account* data monitor is located on the bottom left of the dashboard, with horizontal bars displaying the count of failed logins by user account, with highest count at the top.

Further investigations on the data monitor:

- **Is a particular login account really being used by the brute force attack attempt?** You can check which accounts were heavily used in all attacker systems to access the target systems within the last 24 hours, as follows:
  - Right-click a bar on the graph and select **Show Events**. This opens an active channel using the filter conditions used to construct the selected bar's values specific to the user account. The channel includes the particular correlation event on the user account, attacker address, and target

address.

- Right-click a bar on the graph and select **Investigate**. Select an option to suit your investigative needs. An active channel is displayed based on your selected option. Refer to the *ArcSight Console User's Guide*'s topic, "Choosing Active Channel Menu Commands" for more information.

- **Do you have an external system to help you investigate further?**

  Right-click on a bar and select **Export**. Then select one of the available export options. Refer to the *ArcSight Console User's Guide*'s topic, "Exporting Events to a File," for more information.

To fine tune the *Security Indicator - Failed Login Accounts Count by User Account* data monitor:

ArcSight ESM provides filters to refine the data returned by the data monitor. The data monitor itself has default parameters that determine the time buckets.

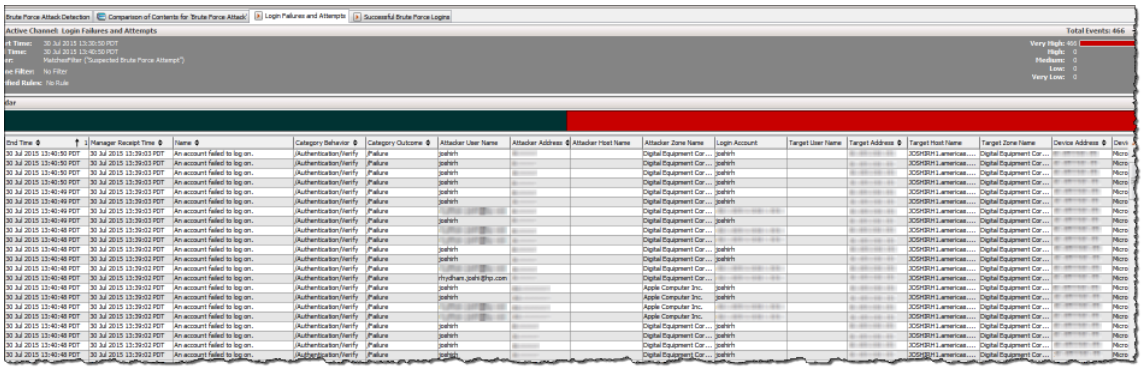
Caution: If making changes to any parameters, you must be familiar with factors that affect ESM performance resulting from these changes. You must also know how to edit ESM resources, such as modifying filter conditions and other attributes. Refer to the *ArcSight Console User's Guide* for details.

Data monitor	• **# Top Entries:** Default is 10. You can increase or reduce this number. • **Bucket Size in Seconds:** Default is 300 seconds (five minutes). You can increase or decrease the number depending on investigative needs. To edit the data monitor, first go to the **Dashboards** resource, then go to the **Data Monitors** tab. The data monitor is located in `/All Data Monitors/Downloads/Hostile Activity Detection/Brute Force Login/Security Indicator - Failed Login Accounts Count by User Account`. The attributes of this data monitor type are described in the *ArcSight Console User's Guide*'s topic on "Top Value Counts Data Monitor" for details.
Filter used by the data monitor	Change the filter conditions to suit your business requirements. The filter is located in `/All Filters/Downloads/Hostile Activity Detection/Brute Force Login/Suspected Brute Force Attempt`. **Caution:** This filter is also used by the other data monitors in the Brute Force Login group. Your changes will therefore impact those data monitors. Refer to the *User's Guide*'s topic on "Filtering Events" for details.

Using the *Login Failures and Attempts* Active Channel

This active channel shows all non-application authentication failures and attempts for last 10 minutes. Use this active channel to monitor user accounts, attacker systems, and target systems used by potential brute force attacks.

Below is an example of the active channel:



To view the active channel:

- On the Brute Force Attack use case's Active Channels section, click the link, **Login Failures and Attempts**.

  Or

- On the ArcSight Console's resource Navigator panel:
  a. Go to `/All Active Channels/Downloads/Hostile Activity Detection`.
  b. Right-click **Login Failures and Attempts** and select **Show Active Channel**.

To use the active channel:

Right-click an item (such as IP address) and select **Show Event Details** to see detailed information about the event. You can also create an inline filter to display events from a specific item. See the *ArcSight Console User's Guide*'s topic on using active channels for information about menu options and inline filters.

Note: The events displayed in an active channel do not refresh automatically at ten-minute intervals. To refresh the view, click the **Stop** and **Replay** channel controls in the toolbar.

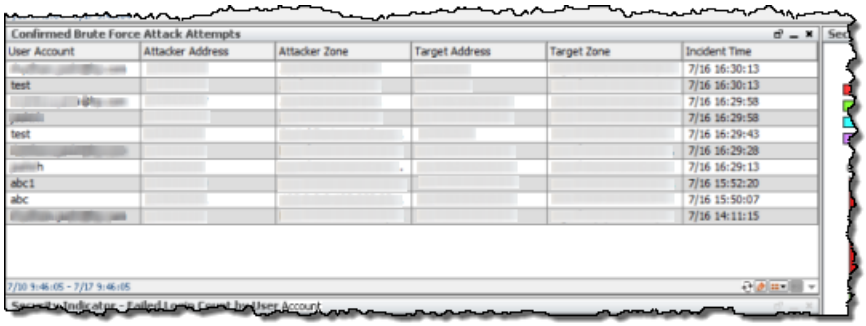
Depending on your environment, ESM load, and specific investigation needs, you can configure an active channel to use continuous, automatic channel refresh: Right-click the link for the active channel in the use case and select **Edit Active Channel**. From the Time Parameters drop-down on the Attributes tab of the Inspect/Edit panel, select **Continuously evaluate**.

Note: In a high EPS environment, you might see performance issues if you scroll down to try and view all the events in the active channel.

Using the *Confirmed Brute Force Attack Attempts* Query Viewer

This query viewer displays information about suspected user accounts, attacker systems, and target systems by running the **Confirmed Brute Force Attack - Attempts** query. The query viewer refreshes every 15 minutes and times out if no results are returned in five minutes.

Following is an example of the query viewer:



The query viewer is located on the left middle section of the dashboard. To refresh this query viewer manually, click the **Refresh** button.

To view the query viewer outside of the dashboard:

- On the Brute Force Attack use case's Query Viewers section, click the link, **Confirmed Brute Force Attack Attempts**.

  Or

- On the ArcSight Console's resource Navigator panel:
  a. Go to `/All Query Viewers/Downloads/Hostile Activity Detection`.
  b. Right-click **Confirmed Brute Force Attack Attempts** and select **View Data as > Table**.

Refer to these topics in the *ArcSight Console User's Guide* for the following information:

- To edit query viewer attributes, refer to the topic, "Defining Query Viewer Settings."
- To edit the query viewer's base query, refer to the topic, "Defining Query Settings." The base query is identified in the query viewer's **Query** field.

  Caution: Before editing a base query, you should know that a base query can be used by other resources, such as reports and trends. Changes to the base query can impact the data displayed on those other resources.

Monitoring Failed Logins from Attacker Systems

One aspect used in brute force investigations is monitoring attacker systems used to access target systems. These attacker systems will show an unusually high number of failed logins within a short duration. When you know of such attacker systems, you can prioritize your responses to protect your assets.

Watching Out for False Positives on Login Failures

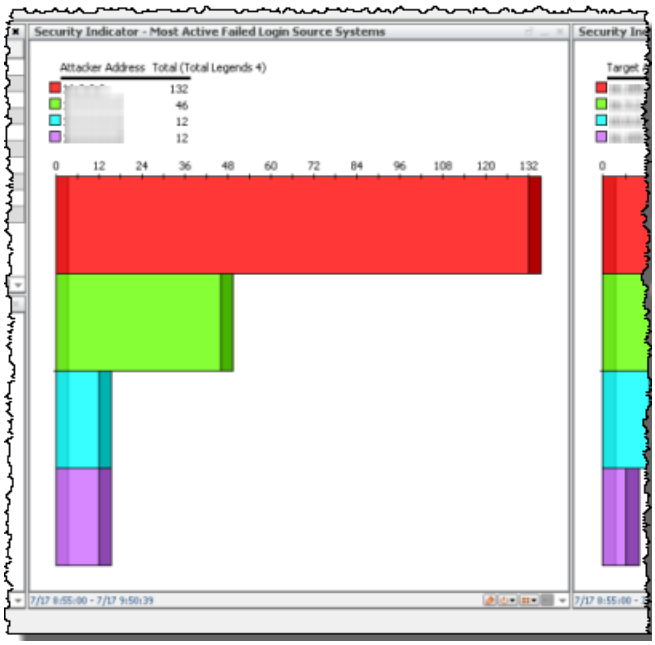
If your environment includes a group of IP addresses specifically used for penetration testing, make sure that these are excluded from the investigation. See "Fine Tuning the Configurations for Monitoring Attacker Systems" on page 26.

Note: Because failed logins contribute to the indicators for the attacker systems used in brute force attempts, it is possible that false positives are being detected. Refer to "Watching Out for False Positives on Login Failures" on page 19 for additional information.

Using the *Security Indicator - Most Active Failed Login Source Systems* Data Monitor

This data monitor tracks the top 10 count of systems from which the brute force attempts are generated. It displays information about attempts grouped by attacker system IP addresses at five-minute intervals over an hour. The display refreshes every 30 seconds. Use this data monitor to determine the most vulnerable systems as the source of the attacks.

Below is a closeup of the data monitor:



To view the data monitor on the dashboard:

- On the Brute Force Attack use case's Monitor section, click the link, **Brute Force Attack Detection**.

  Or
- On the ArcSight Console's resource Navigator panel:
  a. Go to `/All Dashboards/Downloads/Hostile Activity Detection`.
  b. Right-click Brute **Force Attack Detection** and select **Show Dashboard**.

The *Security Indicator - Most Active Failed Login Source Systems* data monitor is located on the lower middle part of the dashboard. The horizontal bars display the count of attacker systems with failed logins, with the highest count at the top.

Further investigations on the data monitor:

- **Investigate particular attacker systems used by the brute force attack attempt.** You can check IP addresses of heavily used attacker systems to access the target systems within the last 24 hours, as follows:
  - Right-click a bar on the graph and select **Show Events**. This opens an active channel using the filter conditions used to construct the selected bar's values specific to the *attacker system*. The channel includes the particular correlation event on the user account, attacker address, and target address.
  - Right-click a bar on the graph and select **Investigate**. Select an option to suit your investigative needs. An active channel is displayed based on your selected option. Refer to the *ArcSight Console User's Guide*'s topic, "Choosing Active Channel Menu Commands" for more information.

- Do you have an external system to help you investigate further?

  Right-click on a bar and select **Export**. Then select one of the available export options. Refer to the *ArcSight Console User's Guide*'s topic, "Exporting Events to a File," for more information.

Fine Tuning the Configurations for Monitoring Attacker Systems

ArcSight ESM provides filters to refine the data returned by the data monitor. The data monitor itself has default parameters that determine the time buckets.

Caution: If making changes to any parameters, you must be familiar with factors that affect ESM performance resulting from these changes. You must also know how to edit ESM resources, such as modifying filter conditions and other attributes. Refer to the *ArcSight Console User's Guide* for details.

Data monitor	• **# Top Entries:** Default is 10. You can increase or reduce this number. • **Bucket Size in Seconds:** Default is 300 seconds (five minutes). You can increase or decrease depending on investigative needs. To edit the data monitor, first go to the **Dashboards** resource, then go to the **Data Monitors** tab. The data monitor is located in `/All Data Monitors/Downloads/Hostile Activity Detection/Brute Force Login/Security Indicator - Most Active Failed Login Source Systems`. The attributes of this data monitor type are described in the *ArcSight Console User's Guide*'s topic on "Top Value Counts Data Monitor" for details.
Filter used by the data monitor	Change the filter conditions to suit your business requirements. For example, your environment may be using a group if IP addresses specifically for penetration testing. You therefore want to exclude that group from the filter. The filter is located in `/All Filters/Downloads/Hostile Activity Detection/Brute Force Login/Suspected Brute Force Attempt`. **Caution:** This filter is also used by other data monitors in the Brute Force Login group. Your changes will therefore impact those data monitors. Refer to the *User's Guide*'s topic on "Filtering Events" for details.

Monitoring Failed Logins to Target Systems

One area used in brute force investigations is monitoring target systems. These target systems will show an unusually high number of failed logins within a short duration. When you know of such target systems, you can prioritize your responses to protect your assets.

Watching Out for False Positives

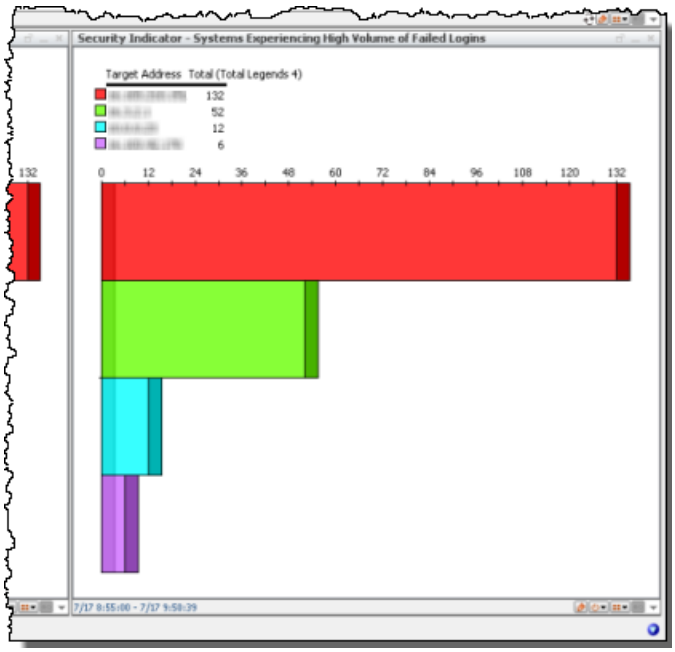
If your environment includes a group of IP addresses specifically used for penetration testing, make sure that these are excluded from the investigation. See "Fine Tuning the Configurations for Monitoring Target Systems" on the next page.

Note: Because failed logins contribute to the indicators for the attacker systems used in brute force attempts, it is possible that false positives are being detected. Refer to "Watching Out for False Positives on Login Failures" on page 19 for additional information.

Using the *Security Indicator - Systems Experiencing High Volume of Failed Logins* Data Monitor

This data monitor tracks the top 10 *target* system IP addresses that reported high rates of login failures. It displays information about the target system IP Address at five-minute intervals over an hour. The display refreshes every 30 seconds. Use this data monitor to determine which systems are the most vulnerable to attacks.

Below is a closeup of the data monitor:



To view the data monitor on the dashboard:

- On the Brute Force Attack use case's Monitor section, click the link, **Brute Force Attack Detection**.

  Or

- On the ArcSight Console's resource Navigator panel:
  a. Go to `/All Dashboards/Downloads/Hostile Activity Detection`.
  b. Right-click **Brute Force Attack Detection** and select **Show Dashboard**.

The *Security Indicator - Systems Experiencing High Volume of Active Failed Login* data monitor is displayed on the lower right corner of the Brute Force Attack dashboard.

Further investigations on the data monitor:

- **Investigate particular target systems used by the brute force attack attempt.** You can check IP addresses of heavily used target systems within the last 24 hours, as follows:
  - Right-click a bar on the graph and select **Show Events**. This opens an active channel using the filter conditions used to construct the selected bar's values specific to the *target system*. The channel includes the particular correlation event on the user account, attacker address, and target address.
  - Right-click a bar on the graph and select **Investigate**. Select an option to suit your investigative needs. An active channel is displayed based on your selected option. An active channel is displayed based on your selected option. Refer to the *ArcSight Console User's Guide*'s topic, "Choosing Active Channel Menu Commands" for more information.
- Do you have an external system to help you investigate further?

  Right-click on a bar and select **Export**. Then select one of the available export options. Refer to the *ArcSight Console User's Guide*'s topic, "Exporting Events to a File," for more information.

Fine Tuning the Configurations for Monitoring Target Systems

ArcSight ESM provides filters to refine the data returned by the data monitor. The data monitor itself has default parameters that determine the time buckets.

Caution: If making changes to any parameters, you must be familiar with factors that affect ESM performance resulting from these changes. You must also know how to edit ESM resources, such as modifying filter conditions and other attributes. Refer to the *ArcSight Console User's Guide* for details.

Data monitor	• **# Top Entries:** Default is 10. You can reduce this number. • **Bucket Size in Seconds:** Default is 300 seconds (five minutes). You can increase or decrease depending on investigative needs. To edit the data monitor, first go to the **Dashboards** resource, then go to the **Data Monitors** tab. The data monitor is located in `/All Data Monitors/Downloads/Hostile Activity Detection/Brute Force Login/Security Indicator - Systems Experiencing High Volume of Failed Logins`. The attributes of this data monitor type are described in the *ArcSight Console User's Guide*'s topic on "Top Value Counts Data Monitor" for details.
Filter used by the data monitor	Change the filter conditions to suit your business requirements. For example, your environment may be using a group if IP addresses specifically for penetration testing. You therefore want to exclude that group from the filter. The filter is located in `/All Filters/Downloads/Hostile Activity Detection/Brute Force Login/Suspected Brute Force Attempt`. **Caution:** This filter is also used by other data monitors in the Brute Force Login group. Your changes will therefore impact those data monitors. Refer to the *User's Guide*'s topic on "Filtering Events" for details.

Fine Tuning Rules for Monitoring Brute Force Attempts

Caution: If making changes to any parameters, you must be familiar with factors that affect ESM performance resulting from these changes. You must also know how to edit ESM resources, such as modifying filter conditions and other attributes. Refer to the *ArcSight Console User's Guide* for details.

The Brute Force Attack use case provides two rules to evaluate and correlate relevant events:

- **Brute Force IDS Detected Attempts** looks for brute force attack attempts detected by the IDS. The rule triggers at the *first receipt* of a brute force attack attempt event from the IDS. On the first event, the user account, attacker system and target system information is added to the **Brute Force Attempts** active list.
- **Brute Force OS and Application Events** looks for brute force attack attempts on OS and applications. The rule triggers when the failed authentication event from the same attacker system using the same user account to the same target system exceeds the threshold, 10 attempts within a minute. On first threshold, information about user account, attacker system and target system is added to the **Brute Force Attempts** active list.

You can edit the rules as follows:

- You can restrict the conditions further to reduce false positives, or loosen up the conditions to reduce false negatives.

- You can modify the aggregation parameters, for example, change the time frame from the default of 1 minute, and also change the number of matches from the default of 10 matches.

Chapter 6: Monitoring Successful Brute Force Attacks

This chapter describes how you, the security analyst, can use the Brute Force Attack use case to monitor successful brute force attacks.

One ESM rule, **Successful Brute Force Login**, to watch for a single successful login attempt that matches any entry in the Brute Force Attempts active list. When the successful login attempt is found, the rule logs the user account, attacker system, and target system information in the **Compromised User Accounts** active list.

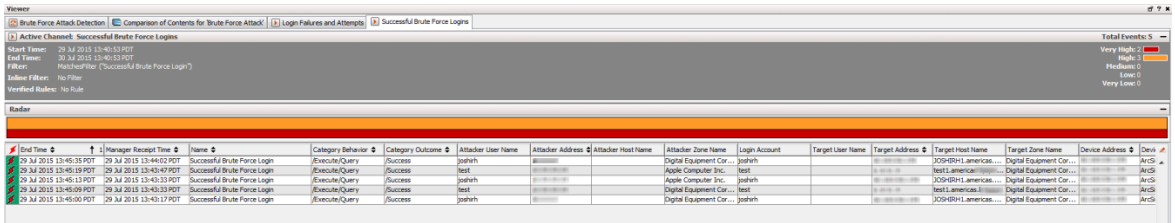
The following topics are covered:

Using the *Successful Brute Force Logins* Active Channel

This active channel displays successful brute force attack correlation events in the past day.

Use this active channel to monitor compromised user accounts and vulnerable assets. Investigate why the user account needs to access the target system and disable the user account. Consider isolating the compromised systems until the threat has been remediated.

Below is an example of the active channel:



To use this active channel:

Right-click an item (such as IP address) and select **Show Event Details** to see detailed information about the event. You can also create an inline filter to display events from a specific item. See the

ArcSight Console User's Guide's topic on using active channels for information about menu options and inline filters.

Note: The events displayed in an active channel do not refresh automatically at ten-minute intervals. To refresh the view, click the **Stop** and **Replay** channel controls in the toolbar.

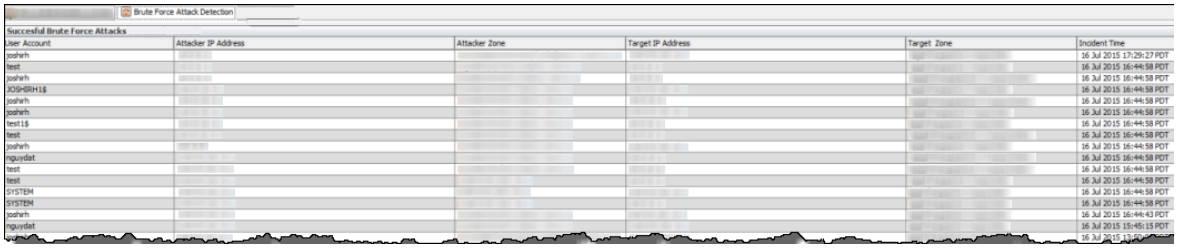
Depending on your environment, ESM load, and specific investigation needs, you can configure an active channel to use continuous, automatic channel refresh: Right-click the link for the active channel in the use case and select **Edit Active Channel**. From the Time Parameters drop-down on the Attributes tab of the Inspect/Edit panel, select **Continuously evaluate**.

Note: In a high EPS environment, you might see performance issues if you scroll down to try and view all the events in the active channel.

Using the *Successful Brute Force Attacks* Query Viewer

This query viewer displays information about compromised users, target systems, and attacker systems by running the **Brute Force Logins - All Compromised Users and Systems** query. The query viewer refreshes every 15 minutes and times out if no results are returned in five minutes.

Following is an example of the query viewer on the Brute Force Attack dashboard:



The query viewer is located at the top of the dashboard.

To view the query viewer outside of the dashboard:

- On the Brute Force Attack use case's Query Viewers section, click the link, **Successful Brute Attacks**.
  Or
- On the ArcSight Console's resource Navigator panel:
  a. Go to `/All Query Viewers/Downloads/Hostile Activity Detection`.
  b. Right-click **Successful Brute Force Attacks** and select **View Data as > Table**.

Refer to these topics in the *ArcSight Console User's Guide* for the following information:

- To edit query viewer attributes, refer to the topic, "Defining Query Viewer Settings."
- To edit the query viewer's base query, refer to the topic, "Defining Query Settings." The base query is identified in the query viewer's **Query** field.

  Caution: Before editing a base query, you should know that a base query can be used by other resources, such as reports and trends. Changes to the base query can impact the data displayed on those other resources.

Fine Tuning the Rule for Monitoring Successful Attacks

By default, the rule called **Successful Brute Force Logins**, located in `/All Rules/Downloads/Hostile Activity Detection`, is designed to add successful brute force events to the **Compromised User Accounts** active list.

Additionally, the rule has the following default but *disabled* actions:

- Create a case in `/All Cases/All Cases/Downloads/Hostile Activity Detection` with the following features:
  - Use a dynamically-configured case name that includes the attacker address, login account, and the target address.
  - Include the base events related to the case.
- Send notification about the successful brute force login to the default destination, `/All Destinations/SOC Operators/`.

  Before modifying the rule action, make sure you have defined your own destination resource if you are not using the default `SOC Operators`.

To enable the rule actions:

Tip: Refer to the ArcSight Console User's Guide, topic on "Rules Authoring," for details on the rule actions described here.

1. Log into the ArcSight Console with administrator privileges.
2. Go to `/All Rules/Downloads/Hostile Activity Detection`, right-click **Successful Brute Force Logins**, and choose **Edit Rule**.
3. Click the disabled rule action, **Add To Existing Case**.
   a. Right-click and choose **Enable Action**.
   b. If you want to further modify the rule action, right-click again and choose **Edit**.

      For example, change the URI if you have previously created a custom case group for brute force attack use.

4. Click the disabled rule action, **Send Notification**.
   a. Right-click and choose **Enable Action**.
   b. If you want to further modify the rule action, right-click again and choose **Edit**.
      For example, choose a different destination group or customize the notification message.

Appendix 1: Brute Force Attack Resource Reference

This appendix lists all the Brute Force Attack resources by type.

Active Channels

The following table lists all the active channels.

Active Channels Resources

Resource	Description	URI
Login Failures and Attempts	This active channel shows all non-application authentication failures and attempts events for last 10 minutes.	`/All Active Channels/Downloads/Hostile Activity Detection/Brute Force Login/`
Successful Brute Force Logins	This active channel displays successful brute force attack correlation events for last 1 day.	`/All Active Channels/Downloads/Hostile Activity Detection/Brute Force Login/`

Active Lists

The following table lists all the active lists.

Active Lists Resources

Resource	Description	URI
Brute Force Attempts	This active list stores information about suspected brute force attempt events. "Brute Force IDS Detected Attempts" and "Brute Force OS and Application Attempts" Rule updates this active list with attacker system, user account and target system information.	`/All Active Lists/Downloads/Hostile Activity Detection/Brute Force Login/`
Compromised User Accounts	This active list stores information about successful brute force attack events. The "Successful Brute Force Login" rule updates this active list with compromised user account, compromised target system and attacker system information details.	`/All Active Lists/Downloads/Hostile Activity Detection/Brute Force Login/`

Dashboards

The following table lists all the dashboards.

Dashboards Resources

Resource	Description	URI
Brute Force Attack Detection	This dashboard presents the complete overview of successful/non-successful and security indicators for successful/suspected Brute Force Attack.	`/All Dashboards/Downloads/Hostile Activity Detection/Brute Force Login/`

Data Monitors

The following table lists all the data monitors.

Data Monitors Resources

Resource	Description	URI
Security Indicator - Failed Login Count by User Account	This data monitor displays top 10 counts of failed authentication events, grouped by user account.	`/All Data Monitors/Downloads/Hostile Activity Detection/Brute Force Login/`
Security Indicator - Most Active Failed Login Source Systems	This data monitor displays top 10 counts of failed authentication events, grouped by attacker IP address.	`/All Data Monitors/Downloads/Hostile Activity Detection/Brute Force Login/`

Data Monitors Resources, continued

Resource	Description	URI
Security Indicator - Systems Experiencing High Volume of Failed Logins	This data monitor displays top 10 counts of failed authentication events, grouped by target IP address.	`/All Data Monitors/Downloads/Hostile Activity Detection/Brute Force Login/`

Global Variables

The following table lists all the global variables.

Global Variables Resources

Resource	Description	URI
Login Account	Login Account/User Account returns "Target User Name" field or "Attacker User Name" field. If "Target User Name" field is not null, this variable returns "Target User Name" field, else it returns "AttackerUserIdCondition" (Local Variable). AttackerUserIdCondition returns "Unknown user", if the "Attacker User Name" field is either null or have value like "null" or "logon", else it returns "Attacker User Name" field.	`/All Fields/Downloads/Hostile Activity Detection/Brute Force Login/`

Field Sets

The following table lists all the field sets.

Field Sets Resources

Resource	Description	URI
Brute Force Login	This field set contains essential fields required to investigate brute force attack through active channels and data monitors.	`/All Field Sets/Downloads/Hostile Activity Detection/Brute Force Login/`

Filters

The following table lists all the filters.

Filters Resources

Resource	Description	URI
Successful Brute Force Login	This filter looks for correlation events generated by the rule: Successful Brute Force Login.	`/All Filters/Downloads/Hostile Activity Detection/Brute Force Login/`
Suspected Brute Force Attempt	This filter looks for all non-successful authentication events.	`/All Filters/Downloads/Hostile Activity Detection/Brute Force Login/`

Queries

The following table lists all the queries.

Queries Resources

Resource	Description	URI
Brute Force Logins - All Compromised Users and Systems	This query returns information about compromised user account, attacker and target systems for last seven days by querying "Compromised User Accounts" active list.	`/All Queries/Downloads/Hostile Activity Detection/Brute Force Login/`
Confirmed Brute Force Attack - Attempts	This query returns information about suspected user account, attacker and target systems for last seven days by querying "Brute Force Attempts" active list.	`/All Queries/Downloads/Hostile Activity Detection/Brute Force Login/`

Query Viewers

The following table lists all the query viewers.

Query Viewers Resources

Resource	Description	URI
Confirmed Brute Force Attack Attempts	This query viewer displays information about suspected user accounts, attacker and target systems by running the "Confirmed Brute Force Attack - Attempts" query.	`/All Query Viewers/Downloads/Hostile Activity Detection/Brute Force Login/`
Successful Brute Force Attacks	This query viewer displays information about compromised users, compromised (target) and attacker systems by running the "Brute Force Logins - All Compromised Users and Systems" query.	`/All Query Viewers/Downloads/Hostile Activity Detection/Brute Force Login/`

Rules

The following table lists all the rules.

Rules Resources

Resource	Description	URI
Brute Force IDS Detected Attempts	This rule looks for brute force attack attempts detected by IDS. The rule triggers when ArcSight ESM receives a brute force attack attempt event from IDS. On first event, the user account, attacker system and target system information is added to "Brute Force Attempts" active list.	`/All Rules/Real-time Rules/Downloads/Hostile Activity Detection/Brute Force Login/`
Brute Force OS and Application Attempts	This rule looks for brute force attacks on OS and applications. The rule triggers when the failed authentication event from the same attacker system using the same user account to the same target system exceeds the threshold. On first threshold, information about user account, attacker system and target system is added to "Brute Force Attempts" active list.	`/All Rules/Real-time Rules/Downloads/Hostile Activity Detection/Brute Force Login/`
Successful Brute Force Login	This rule looks for successful authentication event after suspected brute force attempt. The rule triggers when the user account, attacker system and target system information of successful authentication event matches an entry in the "Brute Force Attempts" active list. When the rule is triggered, it sends notification to SOC Operators (this action is deactivated by default), adds the login account, attacker system and target system information to "Compromised User Accounts" active list and the case is created at its default location (this action is deactivated by default).	`/All Rules/Real-time Rules/Downloads/Hostile Activity Detection/Brute Force Login/`

Use Cases

The following table lists all the use cases.

Use Cases Resources

Resource	Description	URI
Brute Force Attack	This use case tracks brute force login attempts and generates alerts for successful brute force attacks.	`/All Use Cases/Downloads/Hostile Activity Detection/`

Send Documentation Feedback

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

Feedback on Security Use Case Guide (ESM: Brute Force Attack 1.0)

Just add your feedback to the email and click send.

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

We appreciate your feedback!