

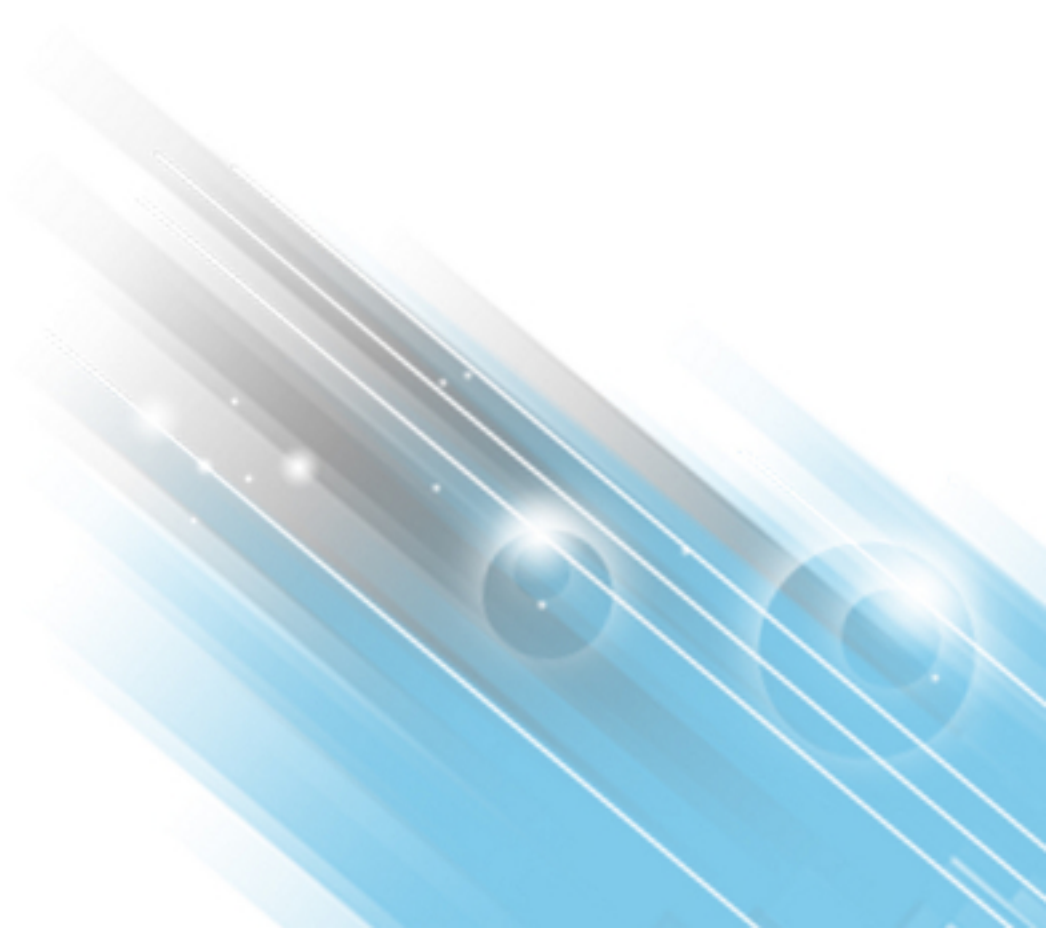


HP ArcSight ESM: VPN Monitoring

Software Version: 1.1

Security Use Case Guide

June 22, 2015



Legal Notices

Warranty

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

The information contained herein is subject to change without notice.

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

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

This document is confidential.

Restricted Rights Legend

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

Copyright Notice

© Copyright 2015 Hewlett-Packard Development Company, L.P.

Follow this link to see a complete statement of copyrights and acknowledgements:

<http://www.hpenterprisesecurity.com/copyright>

Support

Contact Information

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

Contents

Chapter 1: Overview	4
Chapter 2: Installation	6
Importing and Installing a Package	7
Assigning User Permissions	9
Chapter 3: Configuration	10
Chapter 4: Using the VPN Monitoring Use Case	12
Monitoring VPN Login Activity in a Dashboard	13
Investigating VPN Events in an Active Channel	15
Running Reports	17
VPN Monitoring Rules	20
Appendix A: VPN Monitoring Resource Reference	21
Active Channels	21
Dashboards	22
Data Monitors	22
Global Variables	23
Field Sets	23
Filters	24
Queries	25
Reports	26
Rules	27
Session Lists	28
Trends	29
Use Cases	29
Send Documentation Feedback	30

Chapter 1: Overview

A Virtual Private Network (VPN) is the standard for extending your internal network to properly authorized users outside the normal network perimeter. There are potential security risks associated with any VPN implementation.

The VPN Monitoring use case helps you monitor your VPN devices using statistical information about access to critical network assets. You can use this use case for sophisticated data analysis and correlation to detect and analyze security threats, such as network infiltration and data leakage.

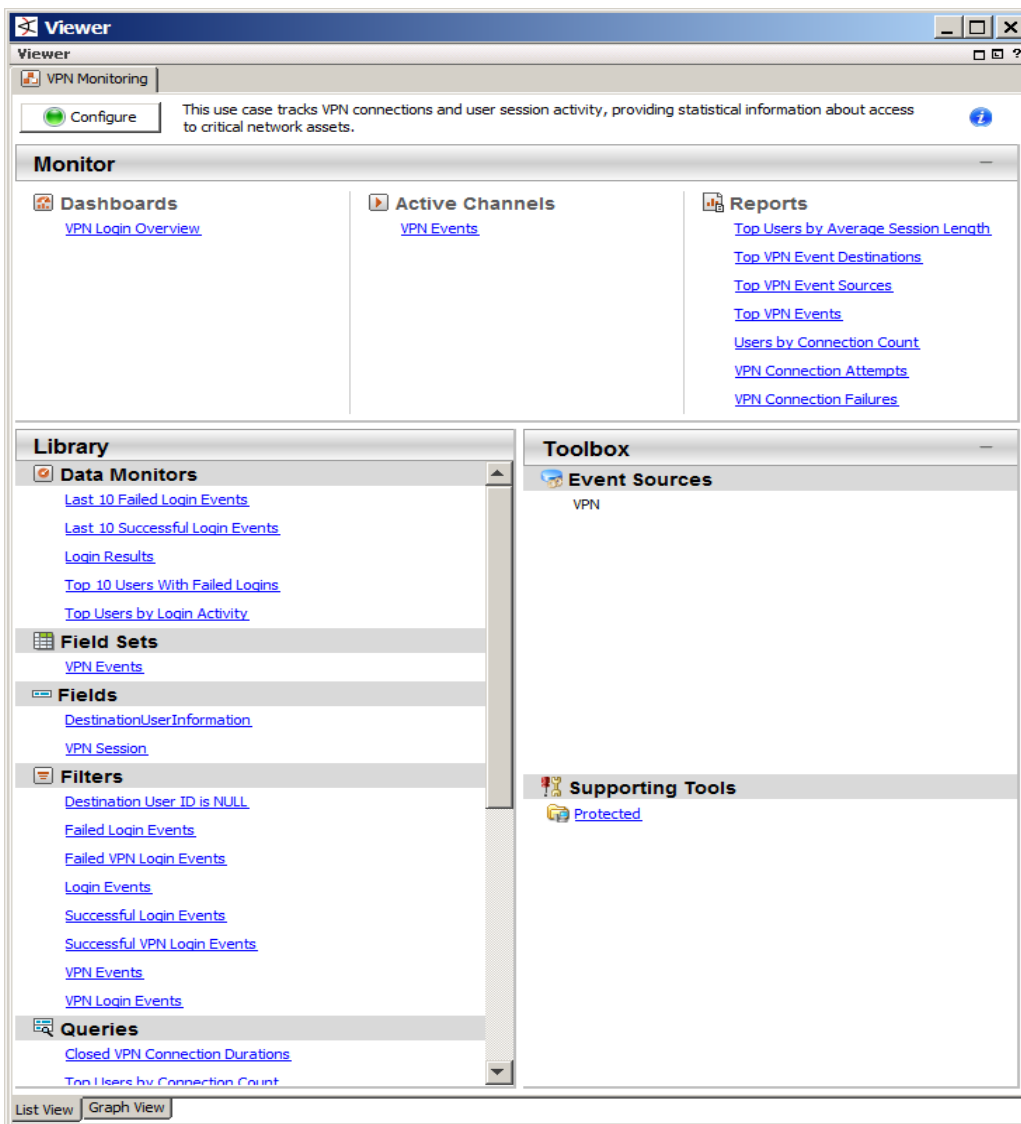
Use the resources in this use case for incident investigation as well as routine monitoring to detect suspicious, abnormal or malicious activity:

- A **dashboard** is provided to show an overview of VPN login activity in real time. You can view the top ten users with the most login activity and the most failed logins, as well as all login results (attempted, successful, and failed) and the last ten failed and the last ten successful login events.
- An **active channel** is provided so that you can investigate all VPN events received within the last ten minutes.
- Several **reports** provide charts and tables showing historical information about the top VPN events, event sources, event destinations, and the top users by average session length. Other reports show the number of VPN connections for each user, and VPN connection attempts and failures.

You can access the **VPN Monitoring** use case from the **Use Cases** tab of the ArcSight Console Navigator panel. The Monitor section of the use case lists the dashboard, active channel, and reports used to monitor traffic and investigate events. The Library section of the use case lists all supporting resources that help compile information in the dashboard, active channel, and reports.

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

The VPN Monitoring use case is shown below.



This document describes how to install, configure, and use the VPN Monitoring use case and is designed for security professionals who have a basic understanding of ArcSight ESM and are familiar with the ArcSight Console. For detailed information about using ArcSight ESM, see the ArcSight ESM documentation set, available as a unified help system from the ArcSight Console **Help** menu. PDF versions of the documentation set, as well as Release Notes, and individual SmartConnector Guides are available from [Protect 724](#).

Chapter 2: Installation

To install the VPN Monitoring use case, perform the following tasks in the order listed.

1. Download the **Downloads Groups** package (Downloads_Groups_1.0.arb) and the **VPN Monitoring** package (VPN_Monitoring_1.1.arb) to the computer where you plan to run the ArcSight Console.

If the Downloads Groups package is already installed on your ArcSight Manager, there is no need to download it again; download the **VPN Monitoring** package only.

Caution: Internet Explorer sometimes converts the .arb file to a .zip file during download. If this occurs, rename the .zip file back to a .arb file before importing.

2. Log into the ArcSight Console with an account that has administrative privileges.
3. Import and install the **Downloads Groups** package. You must import and install this package first.

Note: If the Downloads Groups package is already installed on your ArcSight Manager, you can ignore this step.

4. Import and install the **VPN Monitoring** use case package.
5. Assign user permissions to the VPN Monitoring resources.

The following sections describe how to import and install a package, and how to assign user permissions to the VPN Monitoring resources.

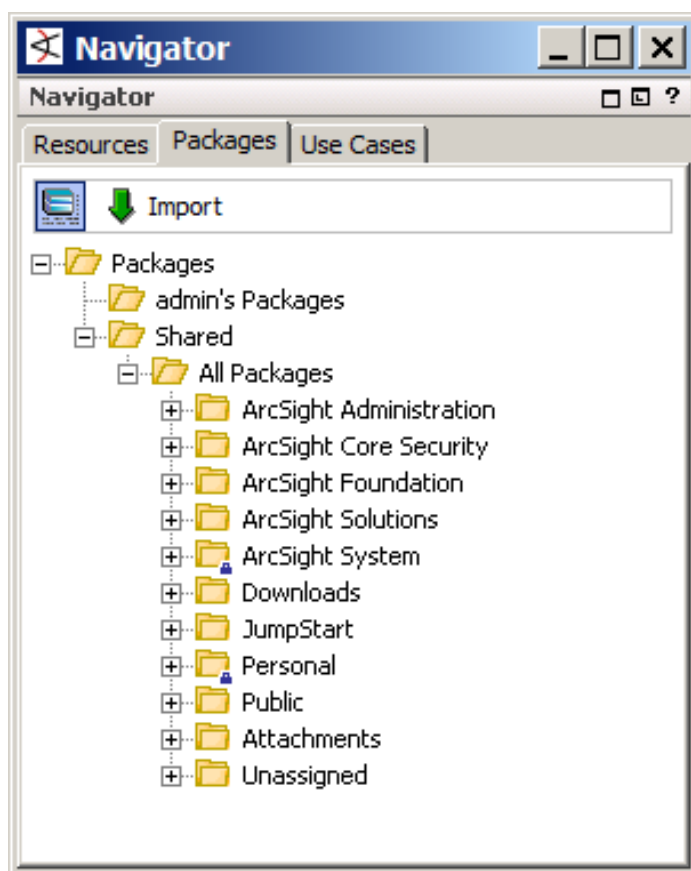
Importing and Installing a Package


Follow the steps below to import and install the **Downloads Groups package** and the **VPN Monitoring use case package**. The Downloads Groups package contains the groups used by the resources in the security use case; you must import and install this package first. After you import and install the Downloads Groups package, follow the same steps to import and install the VPN Monitoring use case package.

Note: If the Downloads Groups package is already installed on your ArcSight Manager, there is no need to install it again; import and install the **VPN Monitoring** package only.

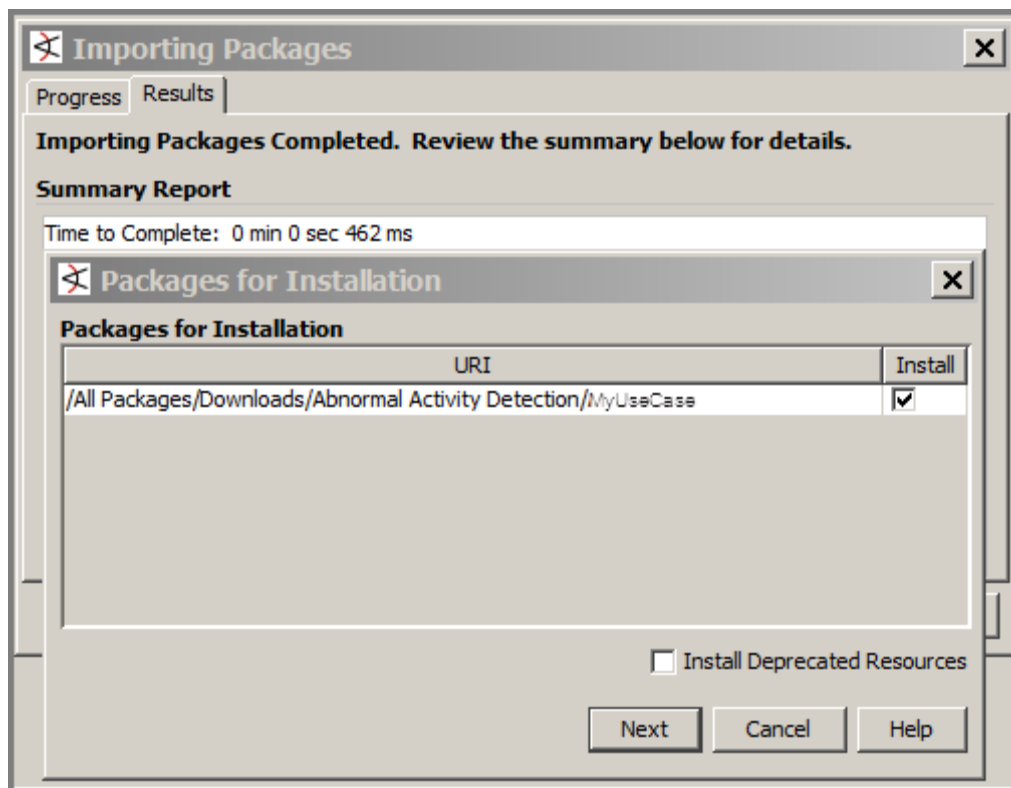
To import and install a package:

1. In the Navigator panel, click the **Packages** tab.



2. At the top of the tab, click  **Import**.
3. In the Open dialog, browse and select the package file you want to import, then click **Open**.

The Progress tab of the Importing Packages dialog shows how the package import is progressing. When the import is complete, the Results tab of the Importing Packages dialog displays together with the **Packages for Installation** dialog. An example is shown below.



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 Installing Packages dialog opens. 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 `Default` user group can view `VPN Monitoring` resources. Users in the `ArcSight Administrators` and `Analyzer Administrators` user groups can view and edit the 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.

The following procedure assumes that you have logged into the ArcSight Console with an account that has administrative privileges, and that you have set up user groups and assigned users to those groups.

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/Network Monitoring`.
3. Right-click the `VPN Monitoring` 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 VPN Monitoring 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 VPN Monitoring use case requires the following configuration for your environment:

- Install the appropriate ArcSight SmartConnectors to receive relevant events. For example, to receive relevant events from Cisco VPN devices, install the SmartConnector for Cisco VPN Syslog.
- Categorize all assets that are internal to the 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). Internal Assets are assets inside the company network. 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.

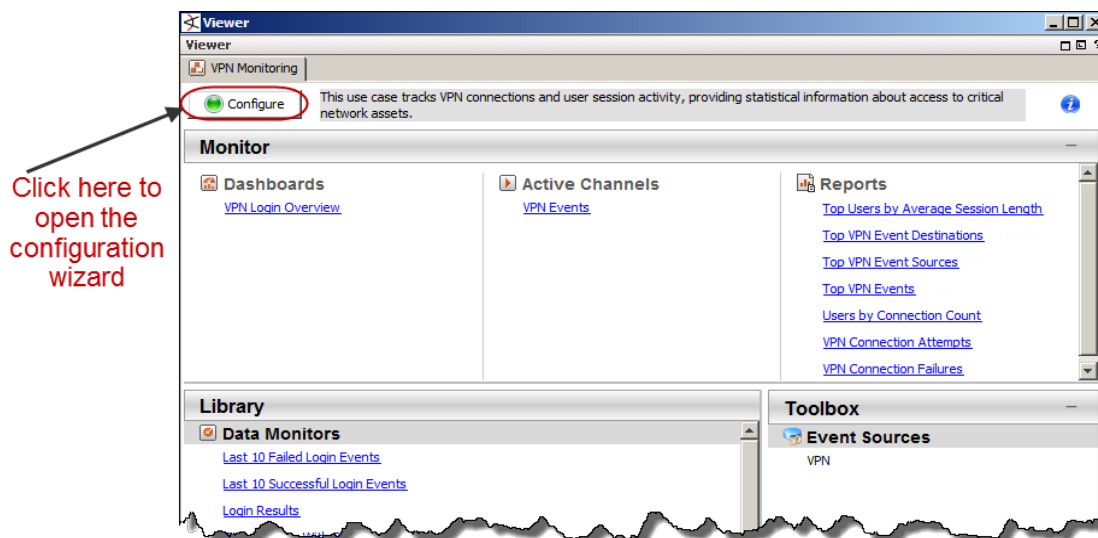
A configuration wizard is provided to guide you through the required configuration. Follow the procedure below.

To configure the VPN Monitoring use case:

1. In the Navigator panel, click the **Use Cases** tab.
2. Browse for the **VPN Monitoring** use case located in /All Use Cases/Downloads/Network Monitoring.
3. Open the VPN Monitoring use case : either double-click the use case or right-click the use case and select **Open Use Case**.

The VPN Monitoring use case lists all the resources used for monitoring VPN activity.

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



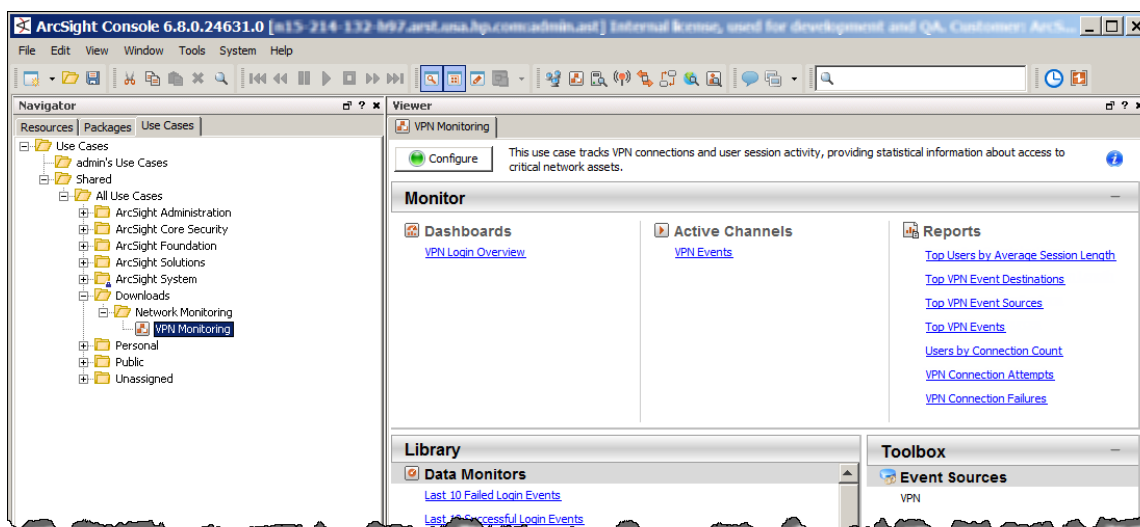
5. Click **Next** to follow the configuration steps.

After you configure the VPN Monitoring use case, you are ready to monitor your VPN devices. See "[Using the VPN Monitoring Use Case](#)" on page 12.

Chapter 4: Using the VPN Monitoring Use Case

The VPN Monitoring use case is located on the **Use Cases** tab in the Navigator panel under /All Use Cases/Downloads/Network Monitoring.

To open the VPN Monitoring use case in the Viewer panel, either double-click the use case or right-click the use case and select **Open Use Case**.



The Monitor section of the VPN Monitoring use case provides resources to help you monitor and investigate VPN-related activity:

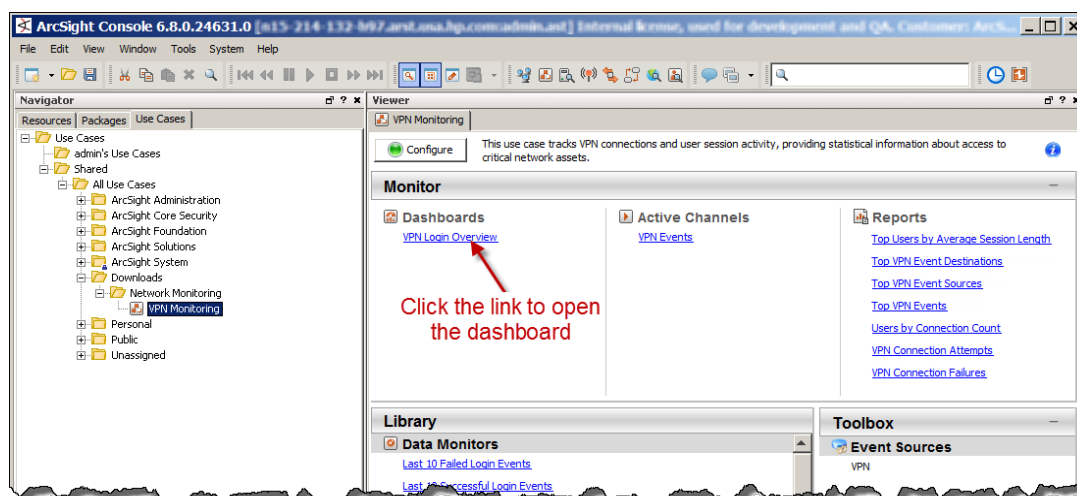
- Use the dashboard to monitor all VPN login activity in real time. See "[Monitoring VPN Login Activity in a Dashboard](#)" on the next page.
- Use the active channel to investigate all VPN events. See "[Investigating VPN Events in an Active Channel](#)" on page 15.
- Run reports that show the top VPN events, event sources, event destinations, and users by average session length. The reports also show the number of VPN connections for each user, and VPN connection attempts and failures. See "[Running Reports](#)" on page 17.

The Library section of the VPN Monitoring use case lists all supporting resources that help compile information in the dashboard, active channel, and reports and includes rules that generate correlated events when triggered. The rules are described in "[VPN Monitoring Rules](#)" on page 20.

Monitoring VPN Login Activity in a Dashboard

The VPN Monitoring use case provides a dashboard to help you monitor VPN login activity in real time. Use the information in the dashboard to look for patterns of use or misuse, or any unusual activity that might indicate potential security concerns.

To open the dashboard, click the link for the **VPN Login Overview** dashboard in the VPN Monitoring use case.

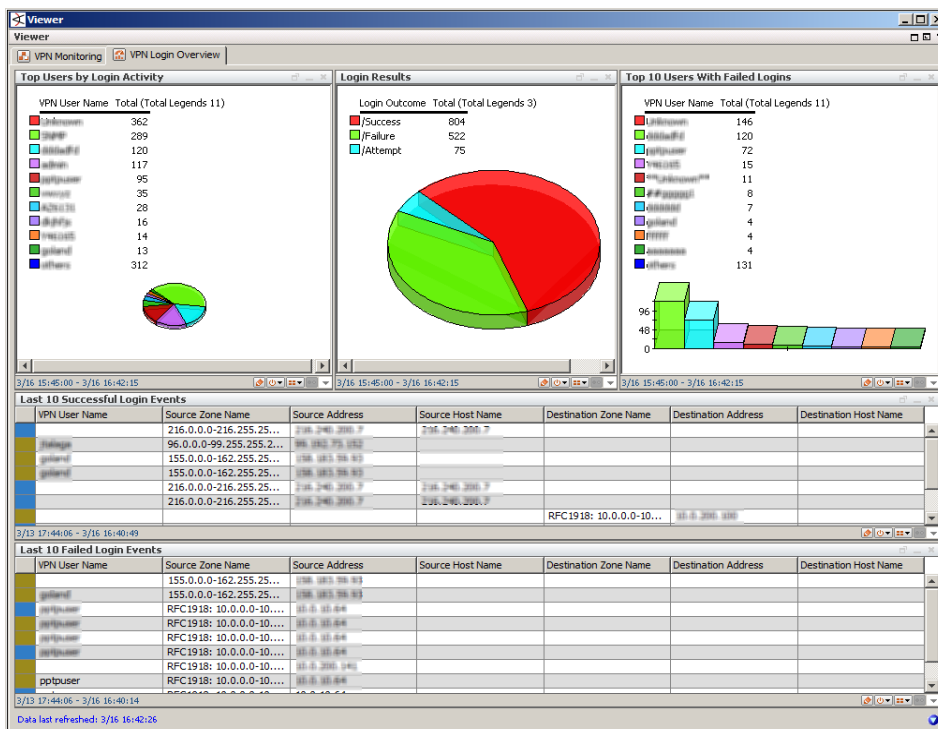


The dashboard opens in the Viewer panel of the ArcSight Console and displays these data monitors:

- **Top Users by Login Activity** displays a pie chart showing the top ten users with the most VPN login activity within the last 60 minutes. Investigate any unusual or excessive login activity by a user as this might indicate a potential security concern. For example, an excessive number of logins by a particular user might indicate that a brute force attack is in progress.
- **Login Results** displays a pie chart showing the number of VPN login attempts, successes, and failures within the last 60 minutes. Examine this data monitor for unusual patterns that might indicate that an attack is being attempted.
- **Top 10 Users With Failed Logins** shows the ten users with the highest number of failed VPN logins within the last 60 minutes. This information is very useful to determine if somebody is trying to compromise your network through your VPN device. Investigate repeated or abnormal failed connections as they might indicate potential attacks.

- **Last 10 Successful Login Events** shows information about the last ten successful logins to a VPN device. You can see the VPN user name, source, destination, and zone information. Watch this activity for any unusual behavior.
- **Last 10 Failed Login Events** shows details about the last ten VPN logins that failed. You can see the VPN user name, the source, destination, and zone information. Investigate multiple failed VPN logins from the same user as this might indicate malicious activity.

An example **VPN Login Overview** dashboard is shown below.



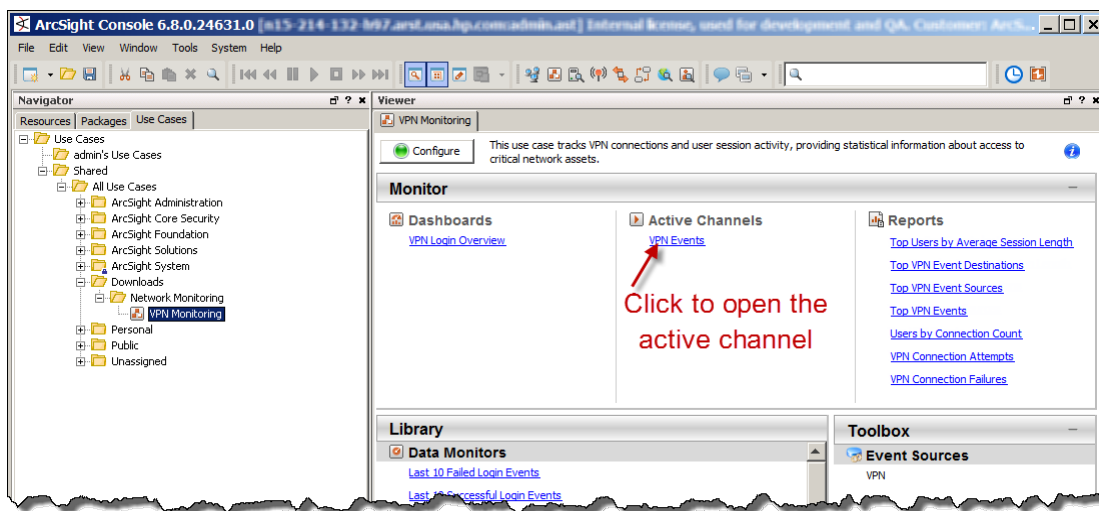
Right-click on an item in a data monitor and select **Investigate > Create Channel** to open an active channel and investigate events further. For example, right-click on a user name in the **Top Users by Login Activity** data monitor and select **Investigate > Create Channel** to open an active channel and investigate the user to obtain details, such as the source IP address and the destination IP address. In the active channel, you can also:

- Create an inline filter to focus on events of interest; for example, you can filter on a specific user name or source address. For detailed information about using inline filters, see the *ArcSight Console User's Guide*.
- Double-click on an event in the active channel to open the event inspector and see details about the event.

Investigating VPN Events in an Active Channel

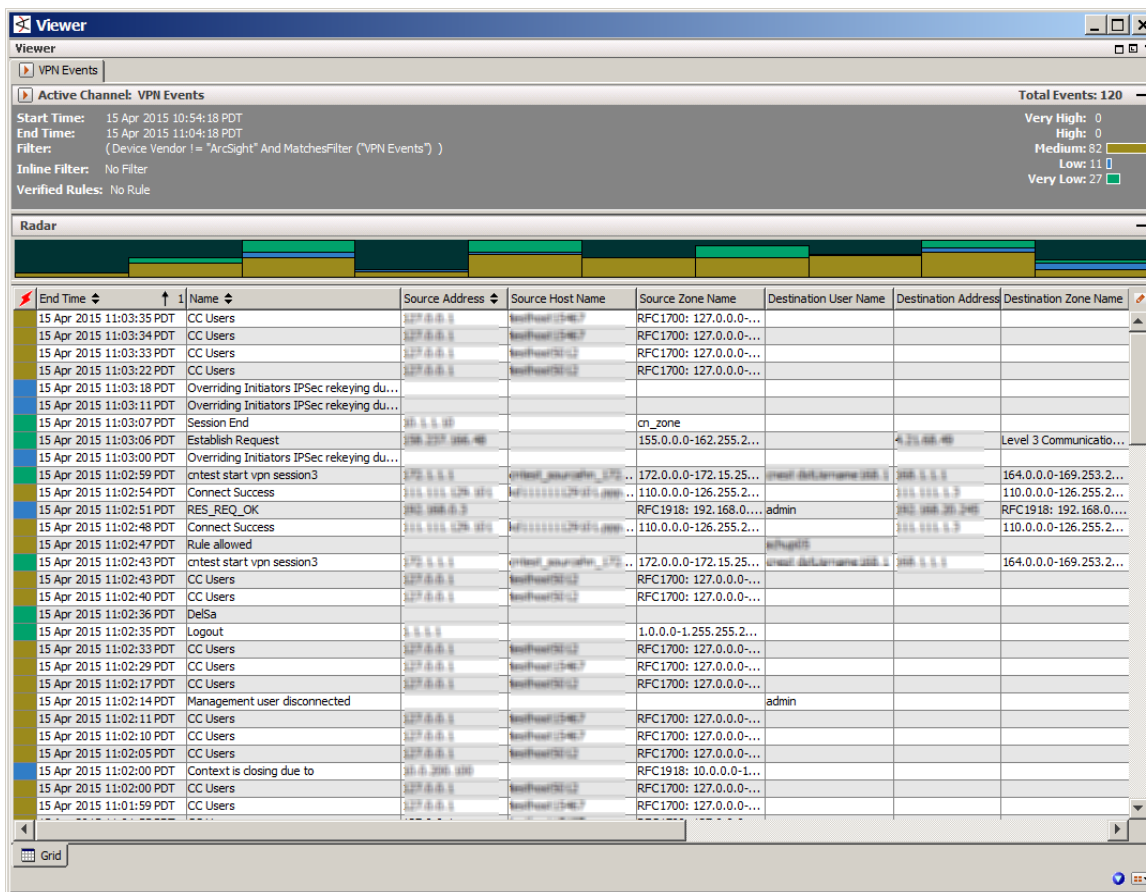
The VPN Monitoring active channel shows all VPN events received within the last ten minutes. Observing and understanding VPN events is essential to the security of your environment and can help you prevent malicious activity and mitigate significant security risks.

To open the active channel, click the **VPN Events** link in the VPN Monitoring use case.



The **VPN Events** active channel opens in the Viewer panel and shows all events received by the ArcSight Manager from VPN devices within the last ten minutes.

An example **VPN Events** active channel is shown below.



Examine these events to spot any unusual patterns involving VPN user logins, and start and terminate VPN sessions. Be sure to investigate events with an ESM priority higher than 7 as this might represent a potential risk to your network. The priority of an event is listed in the Priority column on the far right of the active channel display. You might have to scroll to see the Priority column.

You can 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* for information about creating and using 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.

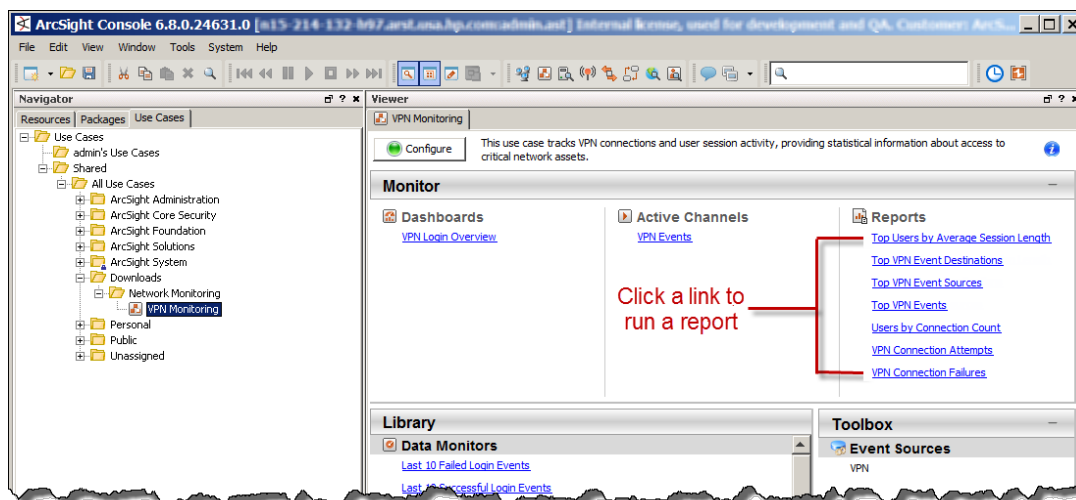
Running Reports

The VPN Monitoring use case provides several reports that you can run to obtain a historical view of your VPN activity graphically in a table or a chart. You can provide these reports to the stakeholders in your company. The reports use VPN device activity information provided by the VPN Connections trend, which runs every day using the VPN Connections - Trend Base query.

By default, the reports use data from the previous day. You can change the start and end time of the report for longer- or shorter-term analysis when you run the report.

To run a report:

1. Click the link for the report in the VPN Monitoring use case.



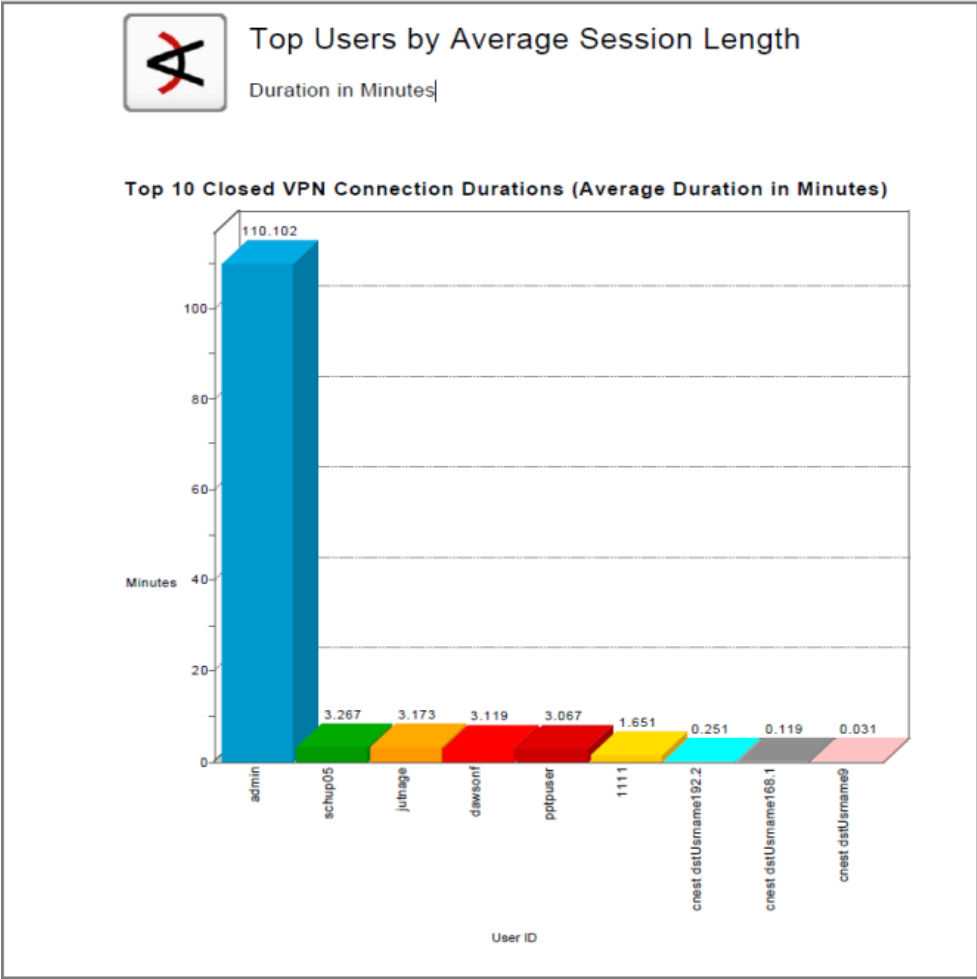
2. In the Report Parameters dialog, set the parameters, then click **OK**. For example, you can change the report format from HTML (the default) to pdf, csv, xls, or rtf, change the page size, and update the report start and end time.

3. For formats other than HTML, either open the report or save the report to your computer when prompted.


The VPN Monitoring use case provides the following reports:

- **Users by Connection Count** shows information about the number of VPN connections for each user. A summary of the users with the most connections is provided. Details of the connections for each user are also provided, including the number of connections and the systems accessed.
- **Top Users by Average Session Length** shows duration information about VPN sessions for each user. A summary of the top VPN connection duration by user is provided. Details of the connection duration for each user are also provided, including minimum, average, maximum, and total connection minutes. Also provided are details about sessions that are currently active at the time the report is run.
- **Top VPN Event Destinations** provides a table showing the IP address, hostname and zone for the top destinations in VPN events, sorted by the number of connections per destination.
- **VPN Connection Attempts** provides a table showing event information where VPN access did not result in failure.
- **Top VPN Event Sources** provides a table showing the IP address, hostname, and zone for the top sources in VPN events, sorted by the number of connections per source.
- **Top VPN Events** provides a table showing the top VPN events (modification events are not included). The table provides the event name, and the source and destination IP address and zone.
- **VPN Connection Failures** provides a table showing information about failed VPN connections. The information includes the VPN user name, source and destination IP address and zone, the VPN device IP address and zone, and the number of failed connections.

An example chart from the Top Users by Average Session Length report is shown below.



VPN Monitoring Rules

The VPN Monitoring use case provides two rules, described below. The rules are deployed in the Real-time Rules group on the Resources tab of the Navigator panel (/All Rules/Real-time Rules/Downloads/Network Monitoring/VPN Monitoring) and enabled by default. The rules trigger when events match one or more set of conditions, at which point a correlation event is generated. A correlation event is displayed in an active channel with the flash icon . Correlation events are fed back into the event life cycle at the ArcSight Manager and are evaluated by both the ArcSight Manager and by the correlation processes. For more information about rule triggering and correlation events, see the *ArcSight Console User's Guide*.

- **User VPN Session Started**

This rule triggers when a VPN user session start event is detected. The rule then creates a new VPN session in the User VPN Sessions and VPN Session by Source IP session lists. This rule supports Cisco VPN products, the Nokia's Security Platform product, and Nortel's VPN product.

- **User VPN Session Stopped**

This rule triggers when a VPN user session terminate event is detected. The rule then terminates the VPN session in the User VPN Sessions and VPN Session by Source IP session lists. This rule supports Cisco VPN products, the Nokia's Security Platform product, and Nortel's VPN product.

Appendix A: VPN Monitoring Resource Reference

This appendix lists all the VPN Monitoring resources by type.

Active Channels	21
Dashboards	22
Data Monitors	22
Global Variables	23
Field Sets	23
Filters	24
Queries	25
Reports	26
Rules	27
Session Lists	28
Trends	29
Use Cases	29

Active Channels

The following table lists all the active channels.

Active Channels Resources

Resource	Description	URI
VPN Events	This active channel shows all VPN activity within the last ten minutes.	/All Active Channels/Downloads/Network Monitoring/VPN Monitoring/

Dashboards

The following table lists all the dashboards.

Dashboards Resources

Resource	Description	URI
VPN Login Overview	This dashboard shows an overview of VPN logins and shows the top users by login activity, the last ten failed login events, the last ten successful login events, login results, and the top ten users with failed logins.	/All Dashboards/Downloads/Network Monitoring/VPN Monitoring/

Data Monitors

The following table lists all the data monitors.

Data Monitors Resources

Resource	Description	URI
Last 10 Failed Login Events	This data monitor shows the last ten failed VPN logins.	/All Data Monitors/Downloads/Network Monitoring/VPN Monitoring/
Last 10 Successful Login Events	This data monitor shows the last ten successful VPN logins.	/All Data Monitors/Downloads/Network Monitoring/VPN Monitoring/
Login Results	This data monitor shows the number of VPN logins (attempt, success, failure) in a pie chart.	/All Data Monitors/Downloads/Network Monitoring/VPN Monitoring/
Top 10 Users With Failed Logins	This data monitor shows the top ten users with failed VPN logins.	/All Data Monitors/Downloads/Network Monitoring/VPN Monitoring/
Top Users by Login Activity	This data monitor shows the users with the most VPN login activity within the last 60 minutes.	/All Data Monitors/Downloads/Network Monitoring/VPN Monitoring/

Global Variables

The following table lists all the global variables.

Global Variables Resources

Resource	Description	URI
DestinationUserInformation	This variable returns VPN user information, which is mapped in VPN events to the Destination User information. The resulting data returned by the variable is either Destination User Name or Destination User ID, whichever is available in the VPN event.	/All Fields/Downloads/Network Monitoring/VPN Monitoring/
VPN Session	This variable retrieves VPN session information from the VPN Session by Source IP session list. The session information is used by the VPN User Activity field set to obtain the VPN user name and by the VPN User Activity active channel to obtain the IP address of the VPN user.	/All Fields/Downloads/Network Monitoring/VPN Monitoring/

Field Sets

The following table lists all the field sets.

Field Sets Resources

Resource	Description	URI
VPN Events	This field set is used by the VPN Events active channel.	/All Field Sets/Downloads/Network Monitoring/VPN Monitoring/

Filters

The following table lists all the filters.

Filters Resources

Resource	Description	URI
Destination User ID is NULL	This filter is used for conditional expression variables. It identifies events in which the Destination User ID is NULL.	/All Filters/Downloads/Network Monitoring/VPN Monitoring/
Failed Login Events	This filter identifies events with the /Authentication/Verify category behavior and the /Failure category outcome.	/All Filters/Downloads/Network Monitoring/VPN Monitoring/
Failed VPN Login Events	This filter identifies failed VPN authentication events.	/All Filters/Downloads/Network Monitoring/VPN Monitoring/
Login Events	This filter identifies events with the /Authentication/Verify category behavior.	/All Filters/Downloads/Network Monitoring/VPN Monitoring/
Successful Login Events	This filter identifies events with the /Authentication/Verify category behavior and the /Success category outcome.	/All Filters/Downloads/Network Monitoring/VPN Monitoring/
Successful VPN Login Events	This filter identifies successful VPN authentication events.	/All Filters/Downloads/Network Monitoring/VPN Monitoring/
VPN Events	This filter identifies events with the /VPN category device group.	/All Filters/Downloads/Network Monitoring/VPN Monitoring/
VPN Login Events	This filter identifies VPN login events.	/All Filters/Downloads/Network Monitoring/VPN Monitoring/

Queries

The following table lists all the queries.

Queries Resources

Resource	Description	URI
Closed VPN Connection Durations	This query identifies the user ID and the minimum, average, maximum, and total durations (in minutes) for all user IDs with closed or terminated VPN sessions in the User VPN Sessions session list.	/All Queries/Downloads/Network Monitoring/VPN Monitoring/
Top Users by Connection Count	This query identifies the top VPN users with the most connection counts, sorted by the number of VPN connections per user.	/All Queries/Downloads/Network Monitoring/VPN Monitoring/
Top VPN Connection Durations	This query identifies the user ID and average duration from the User VPN Sessions session list and sorts them by the top duration.	/All Queries/Downloads/Network Monitoring/VPN Monitoring/
Top VPN Event Destinations	This query identifies the top VPN destinations, sorted by the number of VPN connections per destination.	/All Queries/Downloads/Network Monitoring/VPN Monitoring/
Top VPN Event Sources	This query identifies the top VPN sources, sorted by the number of VPN connections per source.	/All Queries/Downloads/Network Monitoring/VPN Monitoring/
Top VPN Events	This query identifies all events reported by VPN devices, excluding modification events.	/All Queries/Downloads/Network Monitoring/VPN Monitoring/
Users by Connection Count	This query identifies VPN events in which user information is available and returns the user and host information together with the number of VPN connections.	/All Queries/Downloads/Network Monitoring/VPN Monitoring/

Queries Resources, continued

Resource	Description	URI
Users with Open VPN Connections	This query identifies the user ID and the VPN device for each user in the User VPN Sessions session list where the entry for the user has not been terminated (logged out or timed out) or expired (by default).	/All Queries/Downloads/Network Monitoring/VPN Monitoring/
VPN Connection Attempts	This query identifies events where the VPN access did not result in failure.	/All Queries/Downloads/Network Monitoring/VPN Monitoring/
VPN Connection Failures	This query identifies VPN access failure events.	/All Queries/Downloads/Network Monitoring/VPN Monitoring/
VPN Connections - Trend Base	This query is used to populate the VPN Connections trend with the data from various fields in the VPN events.	/All Queries/Downloads/Network Monitoring/VPN Monitoring/

Reports

The following table lists all the reports.

Reports Resources

Resource	Description	URI
Top Users by Average Session Length	This report shows duration information about VPN connections for each user. A summary of the top VPN connection durations by user is provided. Details of the connection durations for each user are also provided, which include the minimum, average, maximum, and total connection minutes. Also included are details of connections that are open at the time the report is run.	/All Reports/Downloads/Network Monitoring/VPN Monitoring/
Top VPN Event Destinations	This report displays a table showing top VPN destinations sorted by connection counts per destination.	/All Reports/Downloads/Network Monitoring/VPN Monitoring/

Reports Resources, continued

Resource	Description	URI
Top VPN Event Sources	This report displays a table showing the top VPN sources, sorted by connection counts per source.	/All Reports/Downloads/Network Monitoring/VPN Monitoring/
Top VPN Events	This report displays a table showing event information reported by VPN devices, excluding modification events.	/All Reports/Downloads/Network Monitoring/VPN Monitoring/
Users by Connection Count	This report shows count information about VPN connections for each user. A summary of the top users by connection count is provided. Details of the connection for each user are also provided, which include connection counts and systems accessed.	/All Reports/Downloads/Network Monitoring/VPN Monitoring/
VPN Connection Attempts	This report displays a table showing event information where VPN access did not result in failure.	/All Reports/Downloads/Network Monitoring/VPN Monitoring/
VPN Connection Failures	This report displays a table showing information about VPN access failures.	/All Reports/Downloads/Network Monitoring/VPN Monitoring/

Rules

The following table lists all the rules.

Rules Resources

Resource	Description	URI
User VPN Session Started	This rule detects a VPN user session start event. The rule then creates a new VPN session in the User VPN Sessions and VPN Session by Source IP session lists. This rule supports Cisco VPN products, Nokia's Security Platform product and Nortel's VPN product.	/All Rules/Real-time Rules/Downloads/Network Monitoring/VPN Monitoring/

Rules Resources, continued

Resource	Description	URI
User VPN Session Stopped	This rule detects a VPN user session terminate event. The rule then terminates the VPN session in the User VPN Sessions and VPN Session by Source IP session lists. This rule supports Cisco VPN products, Nokia's Security Platform product and Nortel's VPN product.	/All Rules/Real-time Rules/Downloads/Network Monitoring/VPN Monitoring/

Session Lists

The following table lists all the session lists.

Session Lists Resources

Resource	Description	URI
User VPN Sessions	This session list tracks VPN user session durations (session starts and stops, or terminations). The default expiration time for a session is five days, at which point the session is considered terminated. If a majority of the sessions are showing a duration of five days, consider increasing the Entry Expiration Time. The sessions are maintained by the User VPN Session Started and User VPN Session Stopped rules.	/All Session Lists/Downloads/Network Monitoring/VPN Monitoring/
VPN Session by Source IP	This session list tracks VPN user sessions with a unique source IP address. The default expiration time for a session is five days, at which point the session is considered terminated. If a majority of the sessions show a duration of five days, consider increasing the Entry Expiration Time. The sessions are maintained by the User VPN Session Started and User VPN Session Stopped rules.	/All Session Lists/Downloads/Network Monitoring/VPN Monitoring/

Trends

The following table lists all the trends.

Trends Resources

Resource	Description	URI
VPN Connections	This trend runs every day and uses the VPN Connections - Trend Base query. The trend table stores data about VPN device activity used in various VPN Monitoring reports.	/All Trends/Downloads/Network Monitoring/VPN Monitoring/

Use Cases

The following table lists all the use cases.

Use Cases Resources

Resource	Description	URI
VPN Monitoring	This use case tracks VPN connections and user session activity, providing statistical information about access to critical network assets.	/All Use Cases/Downloads/Network Monitoring/

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: VPN Monitoring 1.1)

Just add your feedback to the email and click send.

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

We appreciate your feedback!