



**Hewlett Packard**  
Enterprise

# **HPE Security ArcSight DNS Malware Analytics**

Software Version: 2.4

User's Guide

February 8, 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

© Copyright 2017 Hewlett Packard Enterprise Development, LP

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

<https://www.protect724.hpe.com/docs/DOC-13026>

## Support

### Contact Information

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

# Contents

Chapter 1: Introduction .....	1
How DNS Malware Analytics works .....	1
Audience .....	4
Features and benefits .....	4
Workflow summary .....	5
Supported browser .....	9
Changing your profile information .....	9
Setting the time range .....	10
Chapter 2: Managing users .....	12
Database schema information .....	12
Changing your organization name .....	12
Analyzing alerts in ESM .....	12
Adding an analyst .....	13
Changing analyst information .....	14
Chapter 3: Managing DNS Capture Modules .....	15
Appending the blacklist or whitelist .....	15
Naming the DNS Capture Module .....	16
Monitoring DNS packet flow .....	17
Chapter 4: Viewing your network security information .....	19
Understanding suspicious domains and querying client IPs .....	19
Alert types .....	19
Understanding the most queried blacklisted domains .....	20
Top-offending malware types .....	20
Chapter 5: Investigating alerts .....	22
Alert information .....	22
Investigating alert counts .....	23

Filtering alerts .....	24
Exporting alerts .....	25
Chapter 6: Investigating a particular alert .....	26
Opening an alert .....	26
DNS event information .....	26
Investigating DNS events surrounding the alert .....	27
Filtering DNS events .....	29
Chapter 7: Searching DNS records .....	31
Directly investigating an infecting domain .....	31
Directly investigating a suspicious client IP .....	32
Glossary .....	34
Send Documentation Feedback .....	39

# Chapter 1: Introduction

DNS Malware Analytics (DMA) is a scalable, cloud-based threat detector that monitors DNS traffic and rapidly identifies an infected system, enabling immediate remediation in real time. The application can function in a stand-alone configuration as well as in a Security Operations Center (SOC), using HPE - Security ArcSight Enterprise Security Manager (ESM) as the Security Information and Event Management (SIEM) tool.

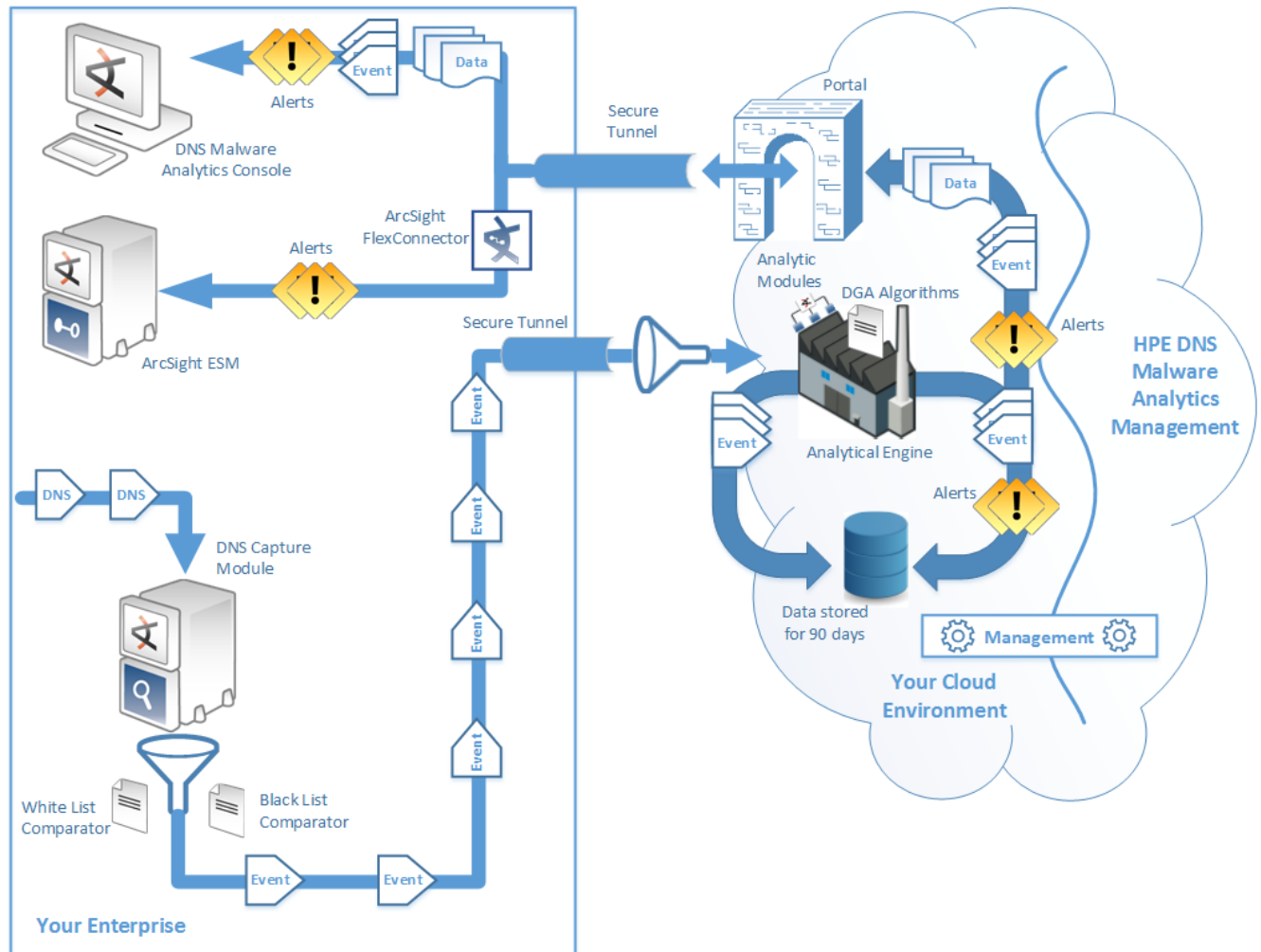
DMA is uniquely differentiated in terms of speed (analyzes billions of DNS packets daily), cloud delivery (cloud-delivered functionality), and scalability with seamless SIEM integration. DMA provides you with an automated infection detection system, allowing enterprises to detect the unknown threats that are the biggest source of risk to enterprise applications, systems, and data.

DMA can detect:

- Blacklist matching — Clients infected with malware that uses blacklisted command-and-control (C&C) domains.
- Botnet to C&C servers — Can be from the client or the domain.
- Cloud platform abuse — Malware infections.
- Standard behavior and conduct violations — Forbidden domains.

## How DNS Malware Analytics works

DNS Malware Analytics (DMA) consists of two analytic platforms. The first is the on-premise DNS Capture Module (DCM) which is a packet-capture device that “listens to” DNS traffic from network links that are connected to internal DNS servers. The second platform is the cloud-based DNS Analytics, which acts as a “black-box” analyzer of DNS events sent from the DCM. These two servers identify infected systems and issues alerts to an upstream SIEM, such as HPE - Security ArcSight Enterprise Security Manager (ESM).



The DCM "sniffs" DNS packets using a TAP (network switch) or SPAN, located between end-point stations and the DNS Server or cluster on the network. The DCM then converts the packets to metadata while discarding packets that are not DNS.

The DCM then filters out "good" DNS queries and responses using a white list comparator. The module only keeps the metadata which is anomalous (suspect or unknown), which is a subset of the overall DNS traffic. (Experience shows that the "good" or discarded traffic is about 99% of the total traffic.)

The anomalous traffic is then passed through another comparator, a blacklist which identifies and labels domain names which are malicious or dangerous. Any remaining anomalous metadata that is unknown is labeled as graylisted.

Next, the DCM converts the anomalous metadata into Common Event Format (CEF) format, to be transported out of the module as DNS events.

The DNS events are sent from the DCM to the DNS Analytical Cloud through a secured tunnel. The DNS events from various DCMs are collected and aggregated in the Analytic Cluster, which is located in a public cloud instance.

The cloud-based Analytical Engine stores the DNS events and also processes them through a set of Analytic Modules, which are a set of plug-ins that provide the intelligence to identify infected clients. These modules are automatically updated by HPE data scientists at regular intervals—and when new threats and conditions are found in the wild. The updated modules are then added to the Analytical Engine so that the latest threat algorithms and detectors are used. You cannot configure the Analytic Modules.

The Analytical Engine can detect seemingly random domain names generated by Domain Generation Algorithms (DGA).

Based on scoring and weighting algorithms, the Analytical Engine generates an alert when an infected IP address is detected. The alert, along with related data (timestamp, alert type, and client IP) can be sent to HPE - ArcSight ESM through the ArcSight Smart Connector for analysis. Other SIEMs can also be used.

### **DMA pages**

DMA enables you to investigate an alert by completing various tasks from the following DMA Console pages:

- **Dashboard** — Comprised of four widgets, which provide overall status of alerts and infections for a selected daily period. Using these widgets, you can learn about infected client IPs, the domains that the malware on the infected systems are trying to contact or are being contacted by malicious domains, and the alerts triggered by DNS events.
- **Alerts** — For a specified time range, displays a summary of alerts that were triggered as the result of infected client IPs. It also displays exactly when an alert occurred and the type of alerts that occurred. It also displays the client IPs that were infected.
- **Alerts > Alert Details** — Shows details around a single IP address (alert). Also provided is a table of triggering DNS events, where the query and response details surrounding a particular alert are given. This includes offending malware, requested domain, event category, and any possible resolution.
- **DNS Finder** — Enables you to search, based on a time period, the entire database in order to discover infected client IPs or suspicious domains. For both of these searches, you can also learn of the alerts and DNS events associated with each. The results of these searches can be filtered by client IPs or domains, depending on the search type.

From the DMA Portal, you can use the following product pages to manage the service:

- **Devices** — Where DCMs are managed. This can include adding content to the blacklist and whitelist, controlling the DNS packet flow from the DCM to the Device Manager, and naming the DCM.
- **Users** — Where users (analysts) are managed. This includes adding analysts and managing their information, along with setting analyst activation. Also from here, the name of the organization can be changed.

The Analytical Cloud—where the Analytical Engine resides, is managed by the HPE DNS Malware Analytics Management Team. While the DMA service retains your data for up to 90 days, in no way can the data be accessed or viewed by anyone but you.

### **Roles and functions**

- HPE administrator — Member of the HPE DNS Malware Analytics Management Team

**Access**

HPE DMA Portal (Customers page and Clusters page)

**Functions**

- Provision (add) and remove SOC administrators in the Analytical Cloud database
- Start and stop the Analytical Cloud
- Enable and update DCMs
- Enable and update Analytics Modules
- View status of processes

- DMA administrator

**Access**

DMA Portal and DMA Console

**Functions**

- Manages the analysts and DCMs of the organization
- Can operate as an analyst
- Add analysts
- Start and stop the DCM
- Modify and update the blacklist and whitelist
- View statuses of processes

- DMA Analysts

**Access**

DMA Console, but not the DMA Portal

**Functions**

- Analyze network activity
- Export alerts (in CVS format)

## Audience

The DNS Malware Analytics documentation is written for security operations staff or analysts working in a medium or large enterprise. It assumes that you are knowledgeable of networks, malware, and DNS concepts.

## Features and benefits

The following are the main features of DNS Malware Analytics (DMA) and their benefits.



- **Find the “bad guys” with threat detection and reduce breach impact**

DNS Malware Analytics identifies infected devices with high fidelity, positively discovering threats on systems, desktop, and mobile devices so they can rapidly be contained. This helps to find the “bad guys” faster by calling out the malware and reducing the impact of breaches by identifying these threats before they gain a foothold inside your network. With look-back capability, sources and spread of malware infections can be identified to reveal threat intent.

- **Faster DNS event resolution**

Enable IT as well as security staff to prioritize and remediate the highest endpoint devices, helping to achieve faster DNS event resolution and contain threats quickly.

- **Lowens monitoring and management costs**

Achieve investigation efficiency by reducing DNS signal noise, enabling organizations to widen their detection footprint, prioritizing, and scoring the critical alerts, which simplifies the alert management process. Removing false positives is a huge time saver for IT staff as well, which saves investigation and staff required to locate infections.

- **Reduces the cost of DNS security**

Lower the cost of DNS security by employing security analytics that help you protect current DNS deployments and help eliminate the costly extraction, backhaul, and processing of DNS server logs.

- **Seamlessly integrates with SIEM to take action on infected hosts**

DMA detects infected hosts enabling customers to utilize their SIEM analytics to get additional detail and take further action to address the threat. It integrates seamlessly with HPE - Security ArcSight Enterprise Security Manager (ESM) by sending alerts in CEF format; ESM enables correlation with other data sources to take action on the alert information.

## Workflow summary

For an administrator, the workflow summary starts from the DNS Malware Analytics (DMA) Portal. Users (analysts) and devices (DNS Capture Modules) are managed from the portal. This includes adding analysts and setting activation, along with managing analyst information. From the portal, you can also change the name of your organization.

For DNS Capture Modules (DCMs), device management includes updating the content to the blacklist and whitelist and managing and monitoring DCM information.

The workflow summary is based on a Dashboard starting point. There could be alternative starting points in the workflow, such as the Alerts page or DNS Finder page.

The following high-level steps cover the functionality of DMA.


1. Launch HPE - ArcSight DNS Malware Analytics from the Chrome web browser.

Use the URL that was sent to you in the "Welcome" email (see ["Supported browser" on page 9](#)).


### Manage users and devices

2. To change the name of your organization, click **Edit** in the Users page (see ["Changing your organization name" on page 12](#)).
3. To access HPE - Security ArcSight Enterprise Security Manager (ESM) for alert analysis, click **Generate Alerts Access Token** in the Users page (see ["Analyzing alerts in ESM" on page 12](#)).  
This task also involves editing the FlexConnector configuration file with the alerts access token and then setting up a channel in ESM for the DMA alerts.
4. To add an analyst, click **Invite User** in the Users page and then specify the email address of the analyst (see ["Adding an analyst" on page 13](#)).

- DMA issues an email to the new analyst for his or her acceptance.
- The registration link in this email is active for only 24 hours from time of issue.
- DMA automatically activates the new analyst.

5. To change analyst information, click  for the desired analyst in the Users page (see ["Changing analyst information" on page 14](#)).

From the Edit User dialog box, you can specify a new analyst email ID and name. You can also activate or deactivate an analyst.

6. To append the blacklist or whitelist with your own content, click the **Whitelist** or **Blacklist** in the Devices page (see ["Appending the blacklist or whitelist" on page 15](#)).
7. To assign a name to the DNS Capture Module, click  in the Devices page for the desired DNS Capture Module (see ["Naming the DNS Capture Module" on page 16](#)).
8. To control DNS packet flow to the DNS Manager, click the desired control button of the Devices page (see ["Monitoring DNS packet flow" on page 17](#)).

- DMA Portal enables you to stop DNS packet flow to the Device Manager, and restart it again. You can also “reboot” the DNS Capture Module and restart it from a total shutdown.
- DMA monitors the DNS Capture Module, including the send and receive rates of DNS packets, total number of DNS packets sent and received, and time running for the module.

9. If you need to contact Technical Support, retrieve your database schema name from the Users page and keep it available (see ["Database schema information" on page 12](#)).

### Specify a time period for analysis

- Specify the period you want to investigate (see ["Setting the time range" on page 10](#)).
  - From the Alerts and DNS Finder pages, you can specify a time range by clicking the begin- and end-time fields.
  - From the Dashboard page, you can view application data for any single day by clicking the time field.

### View your network security information

11. From the Dashboard page, view infections on your network.

- From the "Top Domains Shared by Infected Clients" chart, note the most infecting (suspicious) domains and the client IPs that they may have infected (see ["Understanding suspicious domains and querying client IPs" on page 19](#)).

To learn about all the domains that infected a client IP, click the desired client IP address to open the DNS Finder page (see ["Directly investigating a suspicious client IP" on page 32](#)).

To learn about all the client IPs that a domain infected, click the desired suspicious domain to open the DNS Finder page (see ["Directly investigating an infecting domain" on page 31](#)).

- To learn about a blacklisted domain and all the client IPs infected by this domain, access the "Most Queried Blacklisted Domains" list (see ["Understanding the most queried blacklisted domains" on page 20](#)).

The first five domains are the same ones found in the "Most Infecting Domains and Impacted Client IPs" chart.

- To learn about the blacklisted domain and all the client IPs infected by this domain, click the desired domain (see ["Directly investigating an infecting domain" on page 31](#)).
- To learn about the type and amount of malware used by the suspicious domains, view the "Top Malware Types" chart (see ["Top-offending malware types" on page 20](#)).
- To open the Alerts page and view individual alerts, click the desired alert type from the Alert Types list.
- From the "Top Domains Shared by Infected Clients" chart, note the most infecting (suspicious) domains and the client IPs that they may have infected (see ["Understanding suspicious domains and querying client IPs" on page 19](#)).

To learn about all the domains that infected a client IP, click the desired client IP address to open the DNS Finder page (see ["Directly investigating a suspicious client IP" on page 32](#)).

To learn about all the client IPs that a domain infected, click the desired suspicious domain to open the DNS Finder page (see ["Directly investigating an infecting domain" on page 31](#)).

- To learn about a blacklisted domain and all the client IPs infected by this domain, access the "Most Queried Blacklisted Domains" list (see ["Understanding the most queried blacklisted domains" on page 20](#)).

The first five domains are the same ones found in the "Most Infecting Domains and Impacted Client IPs" chart.

- To learn about the blacklisted domain and all the client IPs infected by this domain, click the desired domain (see ["Directly investigating an infecting domain" on page 31](#)).
- To learn about the type and amount of malware used by the suspicious domains, view the "Top Malware Types" chart (see ["Top-offending malware types" on page 20](#)).

- To open the Alerts page and view individual alerts, click the desired alert type from the Alert Types list.

### Investigate alerts

12. From the Alerts page, click the desired alert type or types from the "Alert Types" list to see individual alerts (see ["Alert information" on page 22](#)).
  - From this page, you can see all the alerts that were triggered as the result of infected client IPs. You can drill down on an alert to view all the events that triggered the alert (see ["Investigating a particular alert" on page 26](#)).
  - To investigate alert counts, access the sparkline scale to view the exact time an alert occurred and the bar-chart scale to narrow the range of alert counts (see ["Investigating alert counts" on page 23](#)).
  - To export alerts in CVS format, click **Export** (see ["Exporting alerts" on page 25](#)).
  - The data that DNS Malware Analytics exports is the time the alert occurred, the type of alert, and the client IP. This is the same data that is in the Alerts table of the Alerts page. DNS events are not exported.
13. To view specific alerts, use alert filter criteria to reduce the Alerts list (see ["Filtering alerts" on page 24](#)).

You can filter alerts based on alert type, most infected client IPs, IP classes, and IP subnets.

### Investigate a particular alert

14. To view events and related information for a particular alert, click the desired alert in the Alerts table (see ["Investigating a particular alert" on page 26](#)).
  - From the Alerts > Alert Details page, you can learn about the infected client IP and see the events that triggered an alert (see ["DNS event information" on page 26](#)).

DMA collects all events generated by suspicious client IPs, but lists no more the first 5000 of these.
  - To investigate events surrounding the alert, hover over the desired sparkline to learn about the malware used and the exact time of the event, or click on the desired sparkline to learn additional details about the event (see ["Investigating DNS events surrounding the alert" on page 27](#)).
  - To view specific events, use the event filter criteria in the left panel to reduce the Alerts list (see ["Filtering DNS events" on page 29](#)).

### Search for a DNS record

15. To directly investigate an suspicious domain, specify the domain in the **Search** field of the DNS Finder page (see ["Directly investigating an infecting domain" on page 31](#)).

- To filter an suspicious domain by a client IP, select the desired client IP bar or bars on the left under “Top Unique Host IP”.
  - From the Dashboard, you can discover a suspicious domain (see ["Understanding suspicious domains and querying client IPs" on page 19](#)). But if you know the domain that you want to investigate, you can go directly to the DNS Finder page and specify that domain.
16. To directly Investigate an infected client IP, specify the client IP in the **Search** field of the DNS Finder page (see ["Directly investigating a suspicious client IP" on page 32](#)).
- To filter a client IP by a domain, select the desired domain bar or bars on the left under “Top Unique Domains”.
  - From the Dashboard, you can discover infected client IPs (see ["Understanding suspicious domains and querying client IPs" on page 19](#)). But if you know the client IP that you want to investigate, you can go directly to the DNS Finder page and specify that client IP.

## Supported browser

Use Google Chrome version 42 or greater to run DNS Malware Analytics.

## Changing your profile information

### About

You can change your name, password, user interface background style, timezone, and specify a profile image.


The company name is set by an HPE administrator.

### Procedure

Location: user icon () > Profile > Profile page

1. To change your name, click  for **Name**.

Your email address is your default name.

2. To change your password, click  for **Password**.
3. To change the user interface background style, select the appropriate option for **Theme Style**.
4. To change the timezone, select the appropriate option for **Timezone**.

Application data is based on a time range. DNS Malware Analytics supports local time and

Coordinated Universal Time (UTC). When using the latter, consider the offset hours applied to your timezone when specifying a time range. If hours are added to your timezone (UTC+x), it is possible that data may not be available for the whole time range. Also, alerts may change since the timezone can change while the selected dates remain the same.

5. To specify a profile image, click **Edit Profile Pic**.
  - Any standard image file format is supported.
  - The file size is limited to 300 kilobytes.
6. To change your email address, contact your administrator.

## Setting the time range

### About

Application data is based on a time range. DNS Malware Analytics supports local time format and Coordinated Universal Time (UTC) format. When using the latter, consider the offset hours applied to your timezone when specifying a time range. If hours are added to your timezone (UTC+x), it is possible that data may not be available for the whole time range. Also, alerts may change since the timezone can change while the selected dates remain the same.

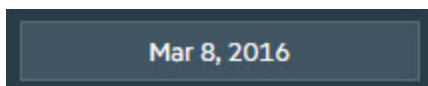
From the Dashboard page, you can view application data for any single day.

From the Alerts and DNS Finder pages, you can view application data for any single day or for multiple days.

### Procedure

Location: Dashboard > Dashboard page

- Click the time field to select a day.



The default is the current day starting at 12:00 AM. The range for the day is from 12:00 AM to the current hour. You cannot change the hour.

Location: Alerts > Alerts page

Other Location

DNS Finder > DNS Finder page

1. Click the begin- and end-time fields to specify a time range.



The range can span up to three months.

2. Specify the day and hour.

**Note:** If you specify a begin time in either the Alerts or DNS Finder page, the Dashboard page will inherit this time. Likewise, if you specify a day in the Dashboard page, the Alerts and DNS Finder pages will inherit this time as the begin time.

#### See Also

["Changing your profile information" on page 9](#)

# Chapter 2: Managing users

Users—analysts, are managed from the DNS Malware Analytics Portal. This includes adding analysts and setting activation, along with managing analyst information. From the DNS Malware Analytics Portal, you can also change the name of your organization.

## Database schema information

Location: Users () > users page

When you purchased DNS Malware Analytics and your account was created, automatically the service created a database schema for you. For technical support purposes, the Users page provides you with the schema name, creation date, and when it was updated.

## Changing your organization name

### Procedure

Location: Users () > users page

1. Click **Edit**.
2. From the Edit Organization Information dialog box, specify your organization name and then click **Save**.

## Analyzing alerts in ESM

### About

To receive alerts in HPE - Security ArcSight Enterprise Security Manager (ESM), an administrator for DNS Malware Analytics (DMA) generates a DMA alert access token. This token is used to configure the ArcSight Common Event Format REST Connector to retrieve alerts from DMA to ESM.

**Note:** If the connector needs to route the web request through a proxy server, a proxy server with or without a username or password may be needed (see the [SmartConnector for ArcSight Common Event Format REST Configuration Guide](#)).

### Procedure



Location: Users () > Users page

1. From the top gray area, click **Generate Alerts Access Token**.
2. From the Alerts Access Token dialog box, click **Copy to clipboard** to capture the DMA-generated token.
3. Install the ArcSight Common Event Format REST Connector as prompted by the install wizard (see the [SmartConnector for ArcSight Common Event Format REST Configuration Guide](#)).
  - The wizard appends the alert access token to the DMA REST API service URL. Copy and paste this entire string in the **Events URL** field of the Parameter Details page of the wizard.

**DMA REST API service URL:**

<https://bd4s.dnsmalwareanalytics.com/api/vertica/retrieveAlerts/>

**Alert access token example:**

JhbGciOiJIUzI1NiJ9.eyJpZCI6MzQsInVzZXJuYWllIjoiYm9vdGNhbXBAYXJjc2lnaHQuY29tIiwiaWF0IjoiJib290Y2FtcEBhcmNzaWdodC5jb20iLCJybzxlIjp7ImlkIjoyLCJuYWllIjoiQWRtaW4ifSwiY3VzdG9tZXIIOnsiaWQiOjExLCJuYWllIjoiSFBFIEFhcmluIiwic2NoZWlhx25hbWUiOiJfRTFvajtBRTV4IiwiiY2xlc3RlciI6eyJlcmwiOiJ2ZXJ0aWNhY2xlc3Rlci5ocG5pZ2h0c3dhdGNoLmNvbSJ9fSwic3ViIjoiSFBUZW5hbnQiLCJhcGlBY2Nlc3MiOiJnZXRBBGVydHMiLCJpYXQiOiJ0NDZAZDNDYWZUsImV4cCI6MTUwMTg4MjAzNX0.MIB0FC7Xc5YGHyLSPLmLev

- The wizard writes the resulting configuration to the `agent.properties` file.
4. Set up an active channel in ESM or use an existing one to view DMA alerts (see the [ESM documentation](#)).

## Adding an analyst

## About

An analyst is added to DNS Malware Analytics (DMA) by responding to an email invitation.

## Procedure

Location: Users () > users page

1. Click **Invite User** and then specify the email address of the desired analyst.

DMA issues an email to the new analyst.

2. Have the new analyst click the registration link in the email and complete the necessary information and accept the EULA.
  - The registration link in this email is active for only 24 hours from time of issue.
  - DMA opens in the Dashboard page.

### See Also

["Changing analyst information" below](#)


## Changing analyst information

### About

You can change the first and last name of an analyst. You can also activate and deactivate an analyst. You cannot delete an analyst from DNS Malware Analytics.

### Procedure

Location: Users () > users page > users table

1. Click  for the desired analyst.
2. From the Edit User dialog box, change the desired information and then click **Save**.
  - To activate or deactivate an analyst, click **Activate** or **Inactive**.
  - Deactivating an analyst does not delete this user.

### See Also

["Changing your profile information" on page 9](#)

# Chapter 3: Managing DNS Capture Modules

DNS Capture Modules (DCMs) are managed from the DNS Malware Analytics Portal. This can include adding content to the blacklist and whitelist, controlling the DNS packet flow from the DCM to the Device Manager, and naming the DCM.

## Appending the blacklist or whitelist

### About

Based on a 24-hour update cycle, the cloud-based Device Manager sends blacklist and whitelist content to the DNS Capture Module (DCM). When the Device Manager detects an update to the blacklist or whitelist content, it pushes the content to the DCM at the end of the 24-hour update cycle.

You can append the HPE-supplied blacklist or whitelist content with your own content. The Device Manager will also detect this update and queue the content to be pushed to the DCM at the end of the 24-hour update cycle.

For Device Manager to update the DCM with your blacklist or whitelist content, you have to specify this information directly in DNS Malware Analytics (DMA) or import it using a CSV file.

**Note:** If you want to append the HPE-supplied blacklist or whitelist content with the blacklist or whitelist content from your proxy server or servers, you have to specify this information directly in DMA or by using a CSV file.

### Procedure

Location: Devices > Devices page

1. Click the **Whitelist** or **Blacklist** link.  
The edit dialog box appears.
2. To add one or more domains to the list, click **Add Entry** and then specify the domain name(s).

If the specified domain is an IP address, DMA will check **This is an IP address**.

- To specify the threat level of the domain, use the **Score** slider.
  - Score is only available for blacklist.
  - Score is used by the Analytical Engine and may affect how alerts are generated.
- Click **Save**.

The new domain appears in the "Domain Name" list.

3. To add domains to the list in bulk, click **Upload CSV file** to import a CSV file containing whitelist or blacklist content and then click **Choose File**.

- Ensure that the CSV file contains a header line. Without this, the content of the file may be ignored.

The header consists of two columns for a whitelist CSV file and three columns for a blacklist CSV file.

- The first column can either be a domain name or an IP address
- The second column is a boolean (true or false) value that identifies which choice you specified in the first column.

For header `dnname, isip`, if you specify a domain name, the second column will be `false` since it is not an IP address. The second column would be `true` if you specify an IP address.

- For a blacklist CSV file, the header contains an additional column for the domain or IP address score, in the format of: `dnname, score, isip`
- You can edit the contents of the CSV file directly in the edit dialog box.
- To learn about the content format of the CSV file, click **View Sample**.
- Click **Save**.  
Device Manager appends your content to the HPE-supplied whitelist or blacklist and pushes it to the DCM at the end of the 24-hour update cycle.

4. To change the entry type and score, hover over the entry in the table and then click the edit button.

Score is only available for blacklist.


## Naming the DNS Capture Module

### About

The serial number for the DNS Capture Module (DCM) alone may not be a memorable identifier and a more comprehensive label may be useful. Therefore, you can specify a device name to help you better identify a DCM.

### Procedure

Location: Devices > Devices page

1. Hover over the desired DCM and then click the more button (.
2. From the "Device Information" dialog box, specify the desired name and then click **Save Changes**.
  - The **Created** date is when the DCM initially came online.

- The **Last Updated** date is when the DCM last received a software update or when you changed the DCM name (**Device Tag**).

## Monitoring DNS packet flow

### About


DNS Malware Analytics (DMA) monitors the send and receive rates of DNS packets, total number of DNS packets sent and received, and time running for the DCM.


### Procedure


Location: Devices > Devices page

1. Open the desired DNS Capture Module (DCM).
  - You can have multiple DCMs open at the same time.
  - The status of the DCM can either be running, updating, stopping, stopped or offline.
  - If offline, you cannot control DNS packet flow. See "Troubleshooting the Installation and Setup" in the *DNS Malware Analytics Getting Started Guide*. If you still cannot find your solution, contact Technical Support.
  - The time count is how long the DCM has been running. This number is reset to zero if you force a reconnect or the DCM shuts down.
2. To learn about the DCM, hover over the DCM and then click the more button (⋮).  
See ["Naming the DNS Capture Module" on the previous page](#).
3. To control DNS packet flow, click the desired button.

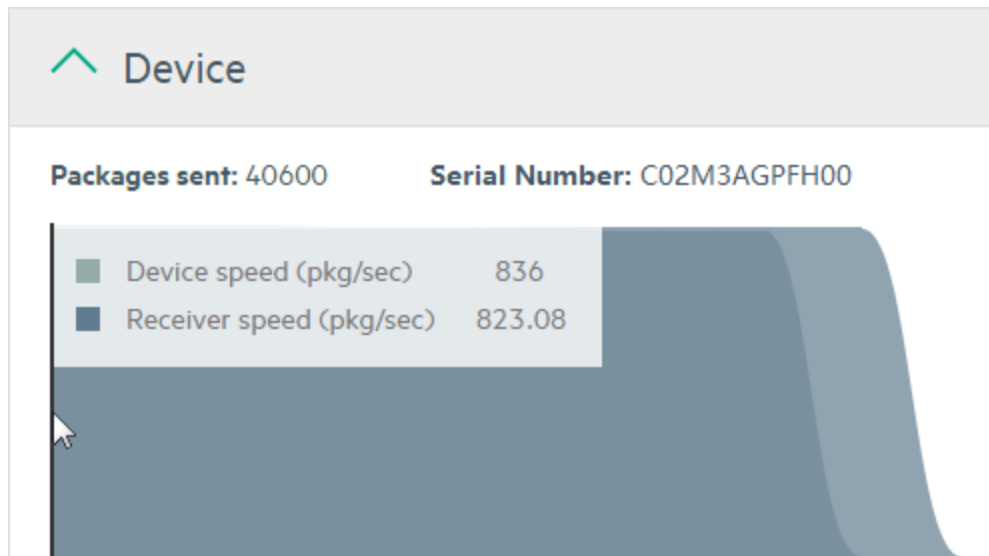
**Note:** Only when the DCM is online and connected with the Device Manager are the control buttons functional.

 — Pauses DNS packet flow from the DCM, while retaining the communication channel between the DCM and the Analytical Cloud.

 — Resumes DNS packet flow to the Device Manager.

 — If the DCM is online and connected, this action will force the DCM to reconnect or "reboot". Also use to restart the DCM from a total shutdown.

4. To learn a rate per second at which the receiver (Analytical Engine) and device (DCM) are processing packets, hover over a desired time segment.



**Packages sent** — DNS packets collected by the DCM and then stored in the DNS Analytical Cloud. This number is relative to the cycle (time). It does not reflect the total of all cycles. If the DCM is disconnected, either by network problems or because you forced it to disconnect, this number will reset.

**Device speed** — The speed at which the DCM sends suspicious DNS records to the Analytical Engine.

**Receiver speed** — The speed at which the Analytical Engine processes DNS records and then writes them to the database.

The graph is updated every second.

**Caution:** In the rare event that DMA (DCM or Cloud or both) is down, you will not see activity in the graph for at least 60 seconds. HPE engineers monitoring the HPE - ArcSight DNS Malware Analytics Management Center in the cloud will correct this situation in a timely manner.

# Chapter 4: Viewing your network security information

The Dashboard provides a good starting point for checking your network.

The Dashboard is comprised of four widgets, which provide alert and infection status for a specific day. From these widgets, you can learn about infected client IPs, the domains and malware used to infect client IPs, and the alerts triggered by DNS events.

## Understanding suspicious domains and querying client IPs

### About

From the "Top Domains Shared by Infected Clients" chart, sparklines connect the most suspicious domains to the client IPs that queried them the most. There can be up to 5 domains and up to 20 client IPs listed in the chart. The domains can be DGA domains or blacklisted domains. The thickness of a sparkline indicates how many events were generated due to the client IP querying specific domain(s).

### Procedure

Location: Dashboard > Dashboard page > Top Domains Shared by Infected Clients

1. To view the number of events generated for a client IP infection, hover over the suspicious domain.
2. To view all the domains that an IP client queried, click the desired client IP (see ["Directly investigating a suspicious client IP" on page 32](#)).
3. To view all the client IPs that queried a suspicious domain, click on the desired domain (see ["Directly investigating an infecting domain" on page 31](#)).

### See Also

["Understanding the most queried blacklisted domains" on the next page.](#)

## Alert types

Location: Dashboard > Dashboard page > Alert Types

Alerts are triggered when a certain amount of DNS events occur. The "Alert Types" list describes the type and amount of alerts that were generated as a result of client IPs attempting contact or contacted by malicious domains.

The following are the possible alert types:

Query Long Domains	Clients made numerous queries to domains with very long names, which may be attempting data extraction over DNS
Query NX DGA	Clients made numerous queries to a domain created by a Domain Generation Algorithm (DGA), but no connection was made (attempted fast flux)
Query Resp DGA	Clients made numerous DNS queries to a domain created by a DGA and at least one reply occurred (fast flux contact)
Query Many Blacklists	Clients attempted to connect to numerous blacklisted domains
Query FBIZeusSink	Clients queried domains associated with Zeus malware that has been flagged by the FBI
Query >50% Blacklists	More than 50% of the DNS queries made by clients were to blacklisted domains
Query 1st Blacklist	A possibly infected client made an attempt to connect to a blacklisted domain.

To view the individual alerts of an alert type, click the desired type (see ["Investigating alerts" on page 22](#)).

## Understanding the most queried blacklisted domains

### About

In the “Most Queried Blacklisted Domains” list, the suspicious domains are listed in descending order of threat score, thereby the number of queries to this domain. The first five domains may be the same ones found in the “Most Infecting Domains and Impacted Client IPs” chart.

The circle containing a number shows the threat score for a particular domain. The number in the center column indicates the total queries made to the domain during the specified day.

### Procedure

Location: Dashboard > Dashboard page > Most Queried Blacklisted Domains

- To learn about a blacklisted domain and all the client IPs infected by this domain, click the desired domain (see ["Directly investigating an infecting domain" on page 31](#)).

### See Also

["Understanding suspicious domains and querying client IPs" on the previous page](#)

## Top-offending malware types

Location: Dashboard > Dashboard page > Top Malware Types

The chart shows the type and amount of malware detected by the Analytic Modules.



The following are the possible malware types:

DGA-Generic	A DGA was detected, but it does not belong to a specific malware family, as indicated by the DMA analytics.
Conficker-AB	Also known as "Downup," "Downadup" and "Kido", is a computer worm targeting the Microsoft Windows operating system that was first detected in November 2008. It uses flaws in Windows OS software and dictionary attacks on administrator passwords to propagate while forming a botnet, and has been unusually difficult to counter because of its combined use of many advanced malware techniques.
Conficker-C	
Unknown-3Lvl	
Blacklist Domains	
Forbidden bigrams	
IP-Domain	
Zeus-Short5TLD	

# Chapter 5: Investigating alerts

An alert is triggered when malware of an infected client IP attempts to ‘phone home’ to a C&C server at a suspicious domain, or when a C&C server replies to the malware DNS query—resulting in events being generated in excess of a limit based on a probability of infection.

## Alert information

Location: Alerts > Alerts page

Other Location

Dashboard > Alert Types > alert type selection > Alerts page

The Alerts page displays the alerts that were triggered as the result of infected client IPs.

The "Alerts" table displays the type of alerts that occurred during the specified time range and exactly when they occurred. It also displays the client IPs that were infected. You can sort each piece of information in ascending or descending order by clicking on the arrows in the column headings. You can also drill down on an alert to view all the events that triggered an alert (see ["DNS event information" on page 26](#)).


If you arrive at the Alerts page from the Dashboard page, only the alerts for the selected alert type are listed in the "Alerts" table. If you go directly to the Alerts page, the "Alerts" table displays alerts for all the alert types for the specified time range.

The "Alert Counts" chart provides two scales that show the amount of alerts that were triggered for a specified time range. The first scale uses bars to represent the quantity of alerts while the other uses sparklines. With your mouse in the chart, you can use the mouse wheel to drill down in the chart.

The following information describes an alert from various perspectives. This information also functions as filter criteria for the "Alerts" table (see ["Filtering alerts" on page 24](#)”).

Alert Types	Alerts are triggered when a certain amount of suspicious DNS events occur. The "Alert Types" list shows the type and number of alerts that were thrown during the specified time range. An alert type can have a sparkline that represents the DNS event count for that type.  See <a href="#">"Alert types" on page 19</a> .
Top IPs	This list ranks—by the number of alerts, the most infected client IPs for the specified time period.

IP Classes	<p>In this list, you can view the number of suspicious client IPs that belong to each IPv4 class—address range. Classes A through D are supported, with Class D being a multicast address range.</p> <p>A sparkline may be associated with a class, showing the alert count for that class.</p>
Top IP Subnets	<p>The first three IPv4 octets of the alert IP address identifies the network subnet.</p> <p>The “Top IP Subnets” list also shows the number of client IPs—by domain, that were infected. These are ranked from the highest to lowest octet: the third IPv4 octet (ex: 192.168.<b>45</b>.x), the second IPv4 octet (ex: 192.<b>168</b>.x.x), and lastly the first IPv4 octet (ex: <b>192</b>.x.x.x).</p>

To further investigate an alert and its related events, click  for the desired alert in the "Alerts" table (see "Opening an alert" on page 26).

## Investigating alert counts

### About

The "Alert Counts" chart provides two scales that show the amount of alerts that were triggered for a specified time range. The first scale—a range selector, uses bars to represent the quantity of alerts while the other uses sparklines.

### Procedure

Location: Alerts > Alerts page > Alert Counts

Other Location:

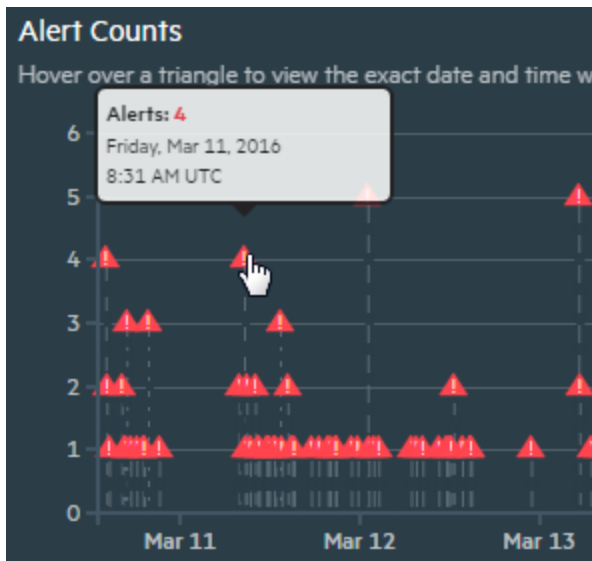
Dashboard > Alert Types > alert type selection > Alerts page > Alert Counts

1. To narrow the range of alert counts, drag the plus cursor (+) across the desired range of the bar-chart scale.

The sparkline scale is reduced to reflect the selected range.



2. To view the exact day and time an alert occurred, hover over the red triangle of the desired sparkline.



3. To view specific alert details, click the red triangle of the desired sparkline.

The "Alerts" table reduces to the alert or alerts of the selected sparkline.

4. To restore the sparklines to the range specified in the time fields, click **Reset** for the "Alerts" table.

## Filtering alerts

### About

You can filter alerts based on alert type, most infected client IPs, IP classes, and IP subnets (see ["Alert information" on page 22](#)). Filtering results in more specific information in the "Alerts" table and in the "Alert Counts" chart.

### Procedure

Location: Alerts > Alerts page

1. Select the desired filter criteria from the left panel (see ["Alert information" on page 22](#)).
  - This selection can be a single criterion or multiple criteria from a single or multiple filter groups.
  - Your filter selection can impact the values of other filter criteria. Whatever filter criteria you select first, determines the available criteria to further narrow your filtering. Subsequent filter selections further reduces the filter criteria values, and can even reduce some to zero.

### Example

If you select the single alert type, “Query NX DGA”, the “Top IPs” list will only contain client IPs for which that alert was triggered. The “IP Classes” list will be adjusted to show the number of times a “Query NX DGA” alert occurred in the listed classes. Likewise, the “Top IP Subnets” list will now reflect the number of times a “Query NX DGA” alert occurred in the various subnets.

**Note:** From the “Alert Counts” chart, you can click the red triangle of the desired sparkline to filter the “Alerts” table to only include the alert or alerts from the selected sparkline (see [“Investigating alert counts” on page 23](#)).

2. To filter the contents of the “Alerts” table, specify your criteria in the **Search** field.
3. To clear the filter criteria, click **Reset** for the “Alerts” table.

If you narrowed the range of alerts in the “Alert Counts” chart, the range selector will be cleared and the chart will include all the sparklines (see [“Investigating alert counts” on page 23](#)).

If you filtered the “Alerts” table based on a sparkline in the “Alert Counts” chart, the table will again include data for the full time range (see [“Investigating alert counts” on page 23](#)).

## Exporting alerts

### About

You can export alerts in CVS format. The data that DNS Malware Analytics (DMA) exports is the time the alert occurred, the type of alert, and the client IP. This is the same data that is in the “Alerts” table of the Alerts page. Events are not exported.

### Procedure

Location:

- Alerts > Alerts page
- Dashboard > Alert Types > alert type selection > Alerts page
- Click **Export**.
  - DMA downloads a CSV file to the Chrome browser download directory.
  - File format example: alerts\_Aug\_3\_\_2015\_9\_00\_PM\_Aug\_4\_\_2015\_9\_00\_PM.csv.

# Chapter 6: Investigating a particular alert

To understand the scope of an alert, view the events that triggered the alert along with the offending domain (or domains) and malware.


## Opening an alert

### About

Drill down on an alert to learn of all the events that triggered the alert, the client IP impacted, and the suspicious domains and malware used by them.

### Procedure

Location: Alerts > Alerts table selection

- Click  in the "Timestamp" column of the desired alert.
  - The alert opens in the Alerts > Alert Details page (see "[DNS event information](#)" below).
  - The selected alert appears in the Alerts drop-down list, identified by its timestamp. Clicking an alert from this drop-down opens the Alerts > Alert Details page where the alert details appear.

## DNS event information

Location: Alerts > Alerts table selection > Alert Details page

From the Alerts > Alert Details page, you can learn about the infected client IP and see the DNS events that triggered an alert. DNS Malware Analytics collects all DNS events generated by suspicious client IPs, but lists no more than the first 5,000 of these. These events can be filtered for specific information.

Event information is presented in chart and table forms.

Events Surrounding the Alert	<p>This chart displays the DNS events (represented by sparklines) that occurred prior to the alert. If any DNS events occurred after the alert, these may also be displayed.</p> <p>The "Events Surrounding the Alert" chart uses color-coded sparklines to correspond to the malwares found in the "Malware Breakdown" list.</p> <p>See <a href="#">"Investigating DNS events surrounding the alert" below</a>.</p>
Events Triggering the Alert	<p>In this table, all the DNS events that are responsible for triggering the alert are listed in time order. The table also displays the suspicious domains, the IP address of the domain if it can be resolved, category of each DNS event, and malware used by the suspicious domain.</p> <p>See <a href="#">"Investigating DNS events surrounding the alert" below</a>.</p>

The "Suspicious Client" area provides the address of the infected client IP that produced the DNS events found in the "Events Surrounding the Alert" chart and "All Events Triggering Alert" table. This area also provides the alert type for the predominant threat, the hostname of the infected client, as well as the time of the alert.

You can click the client IP address to open the DNS Finder page and view the domains that the client IP queried (see ["Directly investigating a suspicious client IP" on page 32](#)).

The following information describes DNS events from various perspectives. This information also functions as filter criteria for the "Events Surrounding the Alert" chart and "Events Triggering the Alert" table (see ["Filtering DNS events" on page 29](#)).

Domain Type	This list displays the type and number of domains that the suspicious client IP queried. The possible domain types are blacklisted, graylisted, and DGA domain.
Categories of DNS Events	This list groups by category the DNS events that triggered the alert.
Malware Breakdown	<p>This list displays all the malware types that the infected client used to connect to its controlling domain. A malware can be a known type or it can be comprised of multiple types to create a unique hybrid.</p> <p>This list also provides the malware rate of occurrence. For example, there may be a total of 50 attempts of Conficker-AB, occurring at intervals of 10 for 5 hours trying to "phone home".</p> <p>When the different components of a malware try to use DNS to contact their master domain, this is reflected in the "Malware Breakdown" list using color codes for malware types that match corresponding DNS event in the "Events Surrounding the Alert" chart.</p>
Suspicious Domains	From this list, the domains most responsible for triggering DNS events are listed. For each domain, the total number of DNS events triggered and their rate per hour are provided.

## Investigating DNS events surrounding the alert

### About

DNS event information is presented in the "Events Surrounding the Alert" chart and the "Events Triggering the Alert" table.

The "Events Surrounding the Alert" chart shows the DNS events (represented by sparklines) that occurred prior to the alert. If any DNS events occurred after the alert, these may also be displayed.

Because a DNS event reflects a type of malware, the "Events Surrounding the Alert" chart uses color-coded sparklines to correspond to the malwares listed in the "Malware Breakdown" list.

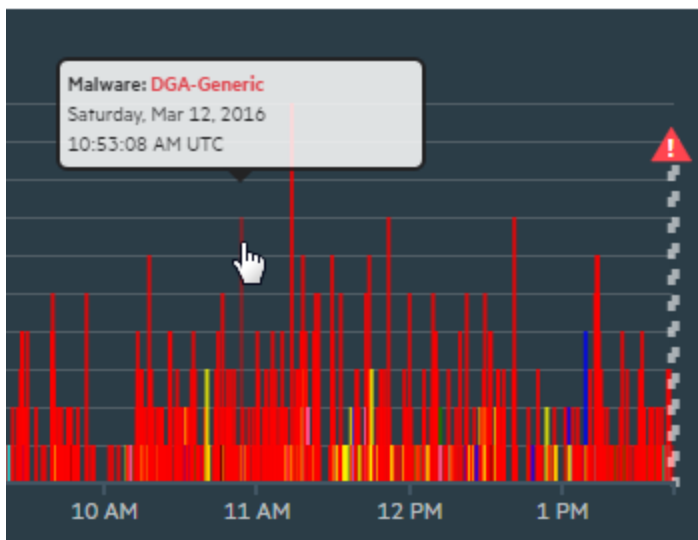
In the "Events Triggering the Alert" table, all the DNS events that are responsible for triggering the alert are listed in time order. The table also displays the suspicious domains, the IP address of the domain if it can be resolved, category of each event, and malware type used by the suspicious domain.

## Procedure

Location:

Alerts > Alerts table selection > Alert Details page > Events Surrounding the Alert

1. To view the malware or malwares that triggered the event and the exact time an event occurred, hover over the desired sparkline.



- The height of an event sparkline indicates (for a particular time segment) the frequency in which malware of an infected client IP was attempting to 'phone home' to a C&C server at a suspicious domain. The sparkline height can also indicate the frequency in which a C&C server was replying to a malware query.
  - In the above example, the malwares (Conficker-AB, SimdaC, and Virut) associated with the event (pink sparkline) occurred a combination of nine times within 12:50 and 12:55.
  - The alert is represented by an exclamation mark (!) within a red triangle.
2. To view specific DNS event details, click the sparkline for the desired event.

The "Events Triggering the Alert" table reduces to the DNS event or events of the selected



sparkline.

3. To drill down in the chart, position your mouse in the chart and scroll with the mouse wheel.

Location: Alerts > Alerts table selection > Alert Details page > Events Triggering the Alert

The "Events Triggering the Alert" table provides the time a DNS event was generated for the client IP, the URL of a suspicious domain, the IP address of a domain if it can be resolved, the suspicious domain category, and the malware used to infect the client IP.

**Note:** If the alert type is Query Resp DGA or Query FBIZeusSink, the associated domain will be resolved. If the alert type is Query NX DGA or Query Many Blacklist, the associated domain will not be resolved. For a NX DGA domain, this is indicated by "NXDOMAIN" appearing in the "Resolution" column. For a Query Many Blacklist domain, this is indicated by "N/A" appearing in the "Resolution" column.

The following are the supported suspicious domain categories:

A	Domain that returns a 32-bit IPv4 address.
AAAA	Domain that returns a 128-bit IPv6 address.
Q	Query
CNAME	Domain with a canonical name using an alias name.
SOA	Domain that specifies authoritative information about a DNS zone, including the primary name server, the email of the domain administrator, the domain serial number, and several timers relating to refreshing the zone.
MX	Mail exchange domain whose name maps to a list of message transfer agents for that domain.
NXDOMAIN	For alert type, Query NX DGA, both the "Resolution" and "Category" columns display "NXDOMAIN".

4. To investigate the domain and infected client IP or IPs behind an event, click the desired domain link.

The DNS Finder page opens (see ["Directly investigating an infecting domain" on page 31](#)).

## Filtering DNS events

### About

You can filter events based on domain type, category of DNS events, malware, and suspicious domains. Filtering results in more specific information in the "Events Triggering the Alert" table and in the "Events Surrounding the Alert" chart.

### Procedure

Location: Alerts > Alerts table selection > Alert Details page

1. Select the desired filter criteria from the left panel (see ["DNS event information" on page 26](#)).
  - This selection can be a single criterion or multiple criteria from a single filter group or groups.
  - Your filter selection can impact the values of other filter criteria. Whatever filter criteria you select first, determines the available criteria to further narrow your filtering. Subsequent filter selections further reduces the filter criteria values, and can even reduce some to zero.

#### Example

If from the "Malware Breakdown" list you select Conficker-AB, which has 16 total occurrences, and from the "Suspicious Domain" list you select `altusnivqq.biz` with a total occurrence of one, one graylist occurrence may be listed under "Domain Type" and one occurrence of NXDOMAIN may be listed under "Categories of DNS Events".

2. To view only the events from a sparkline in the "Events Triggering the Alert" table, click on the desired sparkline.
3. To clear the filter criteria, click **Reset** for the "Alerts" table.

# Chapter 7: Searching DNS records

If you are aware of an suspicious domain or suspicious client IP, DNS Malware Analytics enables you to search for either directly.

## Directly investigating an infecting domain

### About

If you know the domain that you want to investigate, you can go directly to the DNS Finder page and specify that domain. Here, you can discover the client IPs querying or contacted by the domain.

### Procedure

Location: DNS Finder

Other Locations

- Dashboard > Top Domains Shared by Infected Clients
  - Dashboard > Most Queried Blacklisted Domains
  - Alerts > Alerts table selection > Alert Details page > Events Triggering the Alert
1. Accept **Domain** from the **Search** drop-down.
  2. Specify the domain name in the **Search** field and then click **Search**.

The results table provides the time an event was generated for an client IP, the client IP address, whether the subspecies domain is blacklisted, the analytics score of the suspicious domain, whether the domain originated from a Domain Generation Algorithm (DGA), and the suspicious domain category.

Generally speaking, an analytics score of 20 indicates minimal danger, 50 indicates medium danger, and 80 and greater indicates imminent danger.

The following are the supported suspicious domain categories:

A	Domain that returns a 32-bit IPv4 address.
AAAA	Domain that returns a 128-bit IPv6 address.
Q	Query

CNAME	Domain with a canonical name using an alias name.
SOA	Domain that specifies authoritative information about a DNS zone, including the primary name server, the email of the domain administrator, the domain serial number, and several timers relating to refreshing the zone.
MX	Mail exchange domain whose name maps to a list of message transfer agents for that domain.

3. To filter a suspicious domain by a client IP, select the desired client IP bar under “Top Unique Client IP”.
  - The results table is now shorter and only contains occurrences where the specified domain infected the selected client IP.
  - You can select additional domain bars to further filter the search results.
  - You can also filter the results table using the **Search** field.
4. To reset the table to include all client IPs infected by the specified domain, click **Reset**.

#### See Also

["Understanding suspicious domains and querying client IPs" on page 19](#)

## Directly investigating a suspicious client IP

### About

If you know the client IP that you want to investigate, you can go directly to the DNS Finder page and specify that client IP. Here, you can discover the domains that infected the client IP.

### Procedure

Location: DNS Finder > DNS Finder page

#### Other Locations

- Dashboard > Dashboard page > Top Domains Shared by Infected Clients
  - Alerts > Alerts table selection > Alert Details page > Suspicious Client
1. Select **Client IP** from the **Search DNS Records** drop down menu.
  2. Type the IP address in the **Search DNS Records** field and then click **Search**.
    - The results table provides the time an event was generated for the client IP, the domain URL, whether the suspicious domain is blacklisted, the analytics score of the suspicious domain, whether the domain originated from a Domain Generation Algorithm (DGA), and the suspicious domain category.

- Generally, an analytics score of 20 indicates light danger, 50 indicates medium danger, and 80 and greater indicates imminent danger.
- The following are the supported suspicious domain categories:

A	Domain that returns a 32-bit IPv4 address.
AAAA	Domain that returns a 128-bit IPv6 address.
Q	Query
CNAME	Domain with a canonical name using an alias name.
SOA	Domain that specifies authoritative information about a DNS zone, including the primary name server, the email of the domain administrator, the domain serial number, and several timers relating to refreshing the zone.
MX	Mail exchange domain whose name maps to a list of message transfer agents for that domain.

3. To filter a client IP by domain, select the desired domain bar under “Top Unique Domains”.
  - The results table is now shorter and only contains occurrences where the filtered domain infected the specified client IP.
  - You can select additional domain bars to further filter the search results.
  - You can also filter the results table using the **Search** field.
4. To reset the table to include all domains that infected the specified client IP, click **Reset**.

#### See Also

["Understanding suspicious domains and querying client IPs" on page 19](#)

# Glossary

## A

---

### **ArcSight Common Event Format REST Connector**

A SmartConnector that provides a configurable method to collect security events when you use cloud-based application such as DMA. The connector lets ArcSight ESM connect to, aggregate, filter, correlate, and analyze events from applications and devices with CEF standard log output. You can use this powerful, text-based log format to collect logs from customized applications when you modify the output to the CEF standard. See the SmartConnector for ArcSight Common Event Format REST Configuration Guide.

### **ArcSight SmartConnector**

The interface to the objects on your network that generate correlation-relevant event data. After collecting event data from the DNS Collection Module (DCM), they normalize the data in two ways: normalizing values (such as severity, priority, and time zone) into a common format, and normalizing the data structure into a common schema. SmartConnectors can then filter and aggregate events to reduce the volume of events sent to the ArcSight Manager, which increases ESM's efficiency and accuracy, and reduces event processing time. See SmartConnector documentation for complete details.

## B

---

### **Big Data**

Big data is a broad term for data sets so large or complex that traditional data processing applications are inadequate. Challenges include analysis, capture, data curation, search, sharing, storage, transfer, visualization, and information privacy. The term often refers simply to the use of predictive analytics or other certain advanced methods to extract value from data, and seldom to a particular size of data set. Accuracy in big data may lead to more confident decision making. And better decisions can mean greater operational efficiency, cost reduction and reduced risk.

### **Blacklist**

A list of known bad or harmful domains that DNS Malware Analytics uses to identify existing command and control (C&C) domains. This type of domain can be a receiver of infected client communications – a C&C server – in order to further threaten the infected client.

### **Botnet**

A network of computers that have been secretly compromised in order for them to forward transmissions (including spam or viruses) to other computers on the Internet.

## C

---

### **C&C (malware)**

Command and control (C&C) infrastructure consists of servers and other technical infrastructure used to control malware in general, and botnets in particular. C&C servers may be either directly controlled by the malware operators, or themselves run on hardware compromised by malware. Fast-flux DNS can be used as a way to make it difficult to track down the control servers, which may change from day to day. Control servers may also hop from DNS domain to DNS domain, with Domain Generation Algorithms (DGAs) being used to create new DNS names for controller servers.

### **C&C server**

A Command and Control (C&C) server may be either directly controlled by malware operators, or themselves run on hardware compromised by malware. This server is the centralized computer that issues commands to a botnet (zombie army) and receives information back from the malware of an infected client IP.

### **CEF**

Common Event Format (CEF) is an extensible, text-based, high-performance format designed to support multiple device types in the simplest manner possible. Various message syntaxes are reduced to one-matching ArcSight Enterprise Security Manager (ESM) normalization. Specifically, CEF defines a syntax for log records comprised of a standard header and a variable extension, formatted as key-value pairs. This format contains the most relevant event information, making it easy for event consumers to parse and use them. Other standards target a single component of the security infrastructure or are designed for specific applications. These alternatives lack the ability to support today's high-performance, real-time security requirements.

### **CSV Format**

CSV (Comma Separated Values) is a simple file format used to store tabular data, such as a spreadsheet or database. Files in the CSV format can be imported to and exported from programs that store data in tables, such as DMA.

## D

---

### **DGA**

Domain Generation Algorithm (DGA) are algorithms found in various families of malware that are used to periodically generate a large number of apparently random domain names. The command and control (C&C) servers of DGA domains can rendezvous with the domains to gather information that they collected from infected IP clients. The randomness algorithms used by DGA are designed to bypass proxy servers or other suspicious domain-detection software.

### **DGA Domain**

A domain created by a Domain Generation Algorithm (DGA).

### **DNS Event**

An occurrence that reflects an individual DNS query or response. The behavioral analytics detects the most probable type of malware that could be associated with the event.

**DNS Packet**

A suspicious DNS packet collected by the DNS Collection Module is converted into a metadata message and then sent as a DNS event to the DNS Analytical Cloud for analysis.

**DNS Signal Noise**

DNS noise is the normal DNS traffic that is not malicious. The DNS signal is the unknown or suspicious traffic that is potentially malicious.

## E

---

**EULA**

An End User License Agreement (EULA) is a legal contract between you and Hewlett Packard Enterprise regarding the use of DNS Malware Analytics.

## F

---

**Fast Flux**

A DNS technique used by malware to avoid blocking by proxies that use blacklists to detect bad domains. Typically, malware on a client and a malware server on the Internet use a Fast Flux technique to create and communicate over command and control (C&C) channels. Fast Flux uses an algorithm that creates domains that live for short periods of time. For instance, a single domain name can resolve to multiple IP addresses. A DNS query request returns different IP addresses that rotate in a round-robin fashion. If one C&C server (IP) is taken down, the others are still accessible and can be used as C&C servers. Using a similar algorithm in the client malware, enables connections to these short-lived C&C servers in order to pass information. The algorithms used are DGAs.

## G

---

**Graylist**

A list of suspicious or unknown domains that DNS Malware Analytics uses to identify possibly command and control (C&C) domains. At initial analysis, graylist domains cannot be identified as blacklisted or DGA domains.

## H

---

**HPE - Security ArcSight Enterprise Security Manager (ESM)**

A comprehensive software solution—a SIEM that combines traditional security event monitoring with network intelligence, context correlation, anomaly detection, historical analysis tools, and automated remediation. It consolidates and normalizes data from disparate devices across your enterprise network in a centralized view.

## I

---

**IPv4**

Internet Protocol version 4 (IPv4) is the fourth version of the Internet Protocol (IP). It is one of the core protocols of standards-based internetworking methods in the Internet, and was the first version deployed for production in the



ARPANET in 1983. It still routes most Internet traffic today, despite the ongoing deployment of a successor protocol, IPv6. IPv4 is a connectionless protocol for use on packet-switched networks. It operates on a best effort delivery model, in that it does not guarantee delivery, nor does it assure proper sequencing or avoidance of duplicate delivery. These aspects, including data integrity, are addressed by an upper layer transport protocol, such as the Transmission Control Protocol (TCP).

#### **IPv6**

Internet Protocol version 6 (IPv6) is the most recent version of the Internet Protocol (IP), the communications protocol that provides an identification and location system for computers on networks and routes traffic across the Internet. IPv6 provides a larger addressing space. In particular, it permits hierarchical address allocation methods that facilitate route aggregation across the Internet, and thus limit the expansion of routing tables. The use of multicast addressing is expanded and simplified, and provides additional optimization for the delivery of services. Device mobility, security, and configuration aspects have been considered in the design of the protocol. IPv6 is intended to replace IPv4.

## **N**

---

#### **Network Packet Broker**

Network Packet Broker (NPB) is category of compact, hardware-based, rack-mounted devices that offer a new approach for handling and manipulating network packets. NPBs optimize the access and visibility of traffic from one or many network links to monitoring, security and acceleration tools.

#### **NXDOMAIN**

A DNS query status that indicates a non-existent internet domain. The domain name cannot be resolved using DNS servers because the domain name is not registered.

## **S**

---

#### **SIEM**

In the field of computer security, Security Information and Event Management (SIEM) software products and services combine Security Information Management (SIM) and Security Event Management (SEM). They provide real-time analysis of security alerts generated by network hardware and applications. HPE Security ArcSight Enterprise Security Manager (ESM) is an example of a SIEM product.

#### **SOC**

A Security Operations Center (SOC) is a dedicated site where enterprise information systems (websites, applications, databases, data centers and servers, networks, desktops and other endpoints) are monitored, assessed, and defended. A staff supervises the site, using data processing technology.

#### **SPAN**

Most enterprise switches copy the activity of one or more ports through a Switch Port Analyzer (SPAN) port, also known as a mirror port. An analysis device can then be attached to the SPAN port to access network traffic.

#### **Sparkline**

A small line chart, typically drawn without axes or coordinates. It presents the general shape of the variation (typically over time) in some measurement, such as events and alerts, in a simple and condensed way.

## T

---

### **TAP**

A TAP (Test Access Point) is a passive splitting mechanism installed between a 'device of interest' and the network. TAPs transmit both the send and receive data streams simultaneously on separate dedicated channels, ensuring all data arrives at the monitoring device in real time.

### **Task**

An operation where the Device Manager processes DNS events and then writes them to the database.

## U

---

### **UDP Data Protocol**

UDP (User Datagram Protocol) is a session-less method of packet transfer used in the IP data protocol. (DNS usually uses UDP port 53.) UDP is an alternative communications protocol to Transmission Control Protocol (TCP) used primarily for establishing low-latency and loss tolerating connections between applications on the Internet.

### **UTC**

Coordinated Universal Time is the primary time standard by which the world regulates clocks and time. It is, within about 1 second, mean solar time at 0° longitude. It does not observe daylight saving time. It is one of several closely related successors to Greenwich Mean Time (GMT). For most purposes, UTC is considered interchangeable with GMT, but GMT is no longer precisely defined by the scientific community.

## W

---

### **Whitelist**

A list of known domains that DNS Malware Analytics uses to identify domains safe for client IPs to query.

# 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 User's Guide (DNS Malware Analytics 2.4)**

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](mailto:arc-doc@hpe.com).

We appreciate your feedback!