Endpoint Analytics Docs

Release 7.1.5

Plixer, LLC

Apr 20, 2026

VERSION 7.1.5

CHAPTER

ONE

GETTING STARTED

Virtual appliance

Deploy your ESXi virtual appliance

Virtual appliance **Hardware appliance**

Deploy your hardware appliance

Hardware appliance **Appliance setup**

Complete initial setup and licensing after deployment

Appliance setup

CHAPTER

TWO

USING ENDPOINT ANALYTICS

Dashboard

Customizable widgets and at-a-glance system data visualizations

Dashboard **Endpoints**

Inspect and manage endpoint data views, profiles, and download data for offline analysis

Endpoints **Configuration**

Configure and modify Endpoint Analytics' settings

Configuration **Utilities**

Additional tools for performing administrative tasks

Utilities **Reports**

Quick access to predefined reports generated from aggregated endpoint and profile statistics

Reports

CHAPTER

THREE

ADVANCED SERVICES

CLI

beaconctl commands, database operations, and system maintenance functions

Command line operations **REST APIs**

Integrate with Endpoint Analytics using REST API calls

REST APIs **Integrations**

Integrate with Tenable.io, Microsoft Defender, and third-party SSO providers

Integrations **Version Upgrades**

Upgrade procedures and instructions

Version upgrades

CHAPTER

FOUR

HELP AND REFERENCES

FAQs

Answers to frequently asked questions

FAQ **Changelog**

Endpoint Analytics updates and version history

Endpoint Analytics changelogs **Glossary**

Glossary of terms used in Endpoint Analytics

Glossary **Attributions**

Open source and third-party licenses

Third-party attributions About Endpoint Analytics

Endpoint Analytics is a network administration appliance that provides real-time insights into the identities, locations, and behavior of connected devices and enables single pane-of-glass management to enhance security and compliance.

- **Efficient and accurate endpoint identification and management** - The Endpoint Profiling Engine draws on a field-tested library of thousands of predefined profiles to provide administrators with the endpoint information they need when they need it.
- **Continuous endpoint monitoring with real-time alerts** - Endpoint Analytics actively monitors and analyzes network traffic, intelligently identifying rogue devices and suspicious device behavior.
- **Versatile and highly configurable functionality** - Tailor the system to your organization's unique environment with a customizable user interface and granular control over its functions.
- **Scalable, non-intrusive implementation** - Gain visibility over up to tens of thousands of endpoints in any type of enterprise network scenario.
- **Seamless integration with the Plixer family of products** - Gain additional insights with the Risk Intelligence add-on and leverage deep integrations with other products in the Plixer ecosystem to maximize value.

For further questions, check out the *FAQ page* or contact *Plixer Technical Support*.

4.1 Deployment Guides

Endpoint Analytics is available in a deployment package for ESXi environment. Hardware appliance is also available upon request.

On this page:

Pre-deployment *Pre-deployment* Virtual appliance *Virtual appliance* Hardware appliance *Hardware appliance* Basic configuration *Initial configuration*

4.1.1 Pre-deployment

As part of the installation process, the Endpoint Analytics hardware or virtual appliance must be configured with certain information that it needs to interact with the environment it will be deployed to. Certain parts of existing network infrastructure must also be properly configured to allow Endpoint Analytics to collect the data necessary for its functions.

To minimize interruptions during deployment and accelerate the subsequent configuration steps, use the following table to make the necessary preparations beforehand:

Requirement	Description/use
Initial configuration details	Passwords for `beacon` (appliance) and `admin` (web interface) accounts, hostname, management interface (ens160) IP and mask, default gateway IP, name server FQDN or IP, NTP server(s) FQDN or IP; Must be entered during the initial configuration of the hardware or virtual appliance
SSL certificate details	FQDN of the appliance, organization unit and name, state or province, city, and two-letter country code; Will be requested by the initial configuration script for the creation of the self-signed digital certificate and Certificate Signing Request (CSR)
Internal address blocks	Range of endpoint IP addresses to be targeted by the system (typically one or more IP networks or subnets); Must be entered in CIDR (x.x.x.x/mask) format
Network devices	List of network infrastructure devices (NIDs) that will be polled by the system; Must be added via the web interface before Endpoint Analytics can start collecting data from them
SNMP trap information	SNMP trap community string that will be used by NIDs sending traps (NIDs should also be configured to send link state and MAC change traps when possible); Will ensure that only traps from NIDs of interest will be accepted for processing
DHCP traffic visibility	DHCP-addressed endpoints should be configured to have a copy of their traffic redirected to the monitoring port(s) using SPAN, RSPAN, or other mirroring methods; Will allow Endpoint Analytics to analyze traffic between DHCP clients and servers to assign profiles and maintain IP-to-MAC mapping

Note

The items above link directly to the relevant pages under the *Configuration Guides* section of this manual, but reading through this section first is recommended, especially when deploying Endpoint Analytics for the first time.

The default settings of Endpoint Analytics can be further tuned after running the system in production for some time and learning more about the endpoint monitoring requirements for a given enterprise network.

4.1.2 Hardware appliance

After removing the Endpoint Analytics hardware appliance from its packaging, verify that all accompanying accessories (rackmount kit, appliance-locking bezel and keys, and power cord) are included. The appliance can be mounted in a standard 19-inch rack or cabinet.

Important

If your box arrives torn, dented, or otherwise damaged, the appliance itself seems damaged, or there are missing parts, contact *Plixer Technical Support* immediately and **do not attempt to install the unit**.

1. Connect the power cable to the socket in the rear of the appliance and plug the other end into a grounded AC outlet.
2. Connect a monitor, keyboard, and mouse directly to the appliance or through a KVM switch.

> **Hint**
>
> A PC running HyperTerminal can also be used to access the appliance's command line interface (CLI) using serial parameters: 9600 baud, N, 8, and 1.

3. Connect an RJ-45 Ethernet cable to the port labeled **e0:Mgt** behind the appliance and connect the other end of the cable to an available switch port.
4. Connect the monitoring interface(s) to the network switch ports. The second on-board copper port and additional ports in the expansion slots can be used as additional monitor ports for the system.
5. Power on the device using the button on the front panel and use the LEDs to confirm connectivity based on the following table:

LED	State	Connectivity status
Left	Off	No network connection (Link Down)
	Solid amber	Network link established (Link Up)
	Blinking amber	Transmit/receive activity
Right	Off	10 Mbps connection (if left LED is on or blinking)
	Solid amber	100 Mbps connection
	Solid Green	1000 Mbps connection

Once the appliance boots, wait for the login prompt, and then follow the *initial configuration guide* to complete the appliance deployment.

4.1.3 Virtual appliance

To deploy the Endpoint Analytics virtual appliance in ESXi, take note of the following requirements and proceed with the deployment process described below:

- ESXi 6.7 U2+
- VMware vSphere or vCenter
- Resources:
  - Memory: 8 GB
  - Storage: 40 GB
  - CPU: 4 cores, 2.0+ GHz

4.1.3.1 Deploying the OVA template

1. Contact *Plixer Technical Support* and use the link they provide (`https://files.plixer.com/PACKAGE_PATH_AND_FILENAME`) to download the latest VMware virtual appliance package.
2. Extract the contents of the package to a location on the ESXi server.
3. In vSphere or vCenter, right-click the host to deploy the appliance to, and then select **Deploy OVF Template** from the menu.
4. Select **Local file**, and then browse to the Endpoint Analytics OVA file before clicking **Next**.

5. Provide a name for the virtual appliance and continue to follow the deployment wizard.
6. When done, verify the configuration in the summary, and then click **Finish** to import the virtual appliance.

Once the Endpoint Analytics virtual appliance has been imported, right-click on the VM to power it on, and then follow the *initial configuration guide* to complete the deployment process.

By default, the OVF install includes 2 CPUs, 4GB RAM, 40GB storage, and 2 network adapters. In most cases, this configuration is sufficient. However, if you increase your virtual hardware allocation, you must make those changes within your KVM environment (e.g., increasing RAM via VMware), as they cannot be configured through Endpoint Analytics.

4.1.3.2 Adding new interfaces

To add a new interface (for ERSPAN traffic) to the Endpoint Analytics virtual appliance, follow these steps:

1. In vCenter, right click on the Endpoint Analytics VM, and then select **Edit Settings…**.
2. Select **Add New Device**, and then select **Network Adapter** from the dropdown.

After the new interface has been added, it can be *configured to receive ERSPAN traffic* via the web interface.

4.1.4 Initial configuration

After the Endpoint Analytics hardware or virtual appliance has been set up, the system will be ready for initial configuration.

4.1.4.1 Appliance setup

After powering on the Endpoint Analytics appliance for the first time, log in with the credentials `beacon:beacon`, and then wait for the device to reboot.

After logging in again, follow the appliance setup prompts as described below to allow access to the web interface:

1. At the **Welcome** dialog, verify that the version number displayed matches the version you purchased. When done, select **OK**, and then press **Enter** to continue.
2. Enter the following information in the network configuration dialog:
   - System/appliance hostname (will be required by *Plixer Technical Support* for *licensing*)
   - Management interface (ens160) IP address with netmask/CIDR
   - Management interface (ens160) default gateway/router address
   - One or more DNS server IP addresses (comma-separated, without spaces)
   - One or more NTP server FQDNs or IP addresses (comma-separated, without spaces)
3. Verify that all details are correct, and then select **Submit** to save the information and proceed.
4. Continue through the succeeding dialogs, and then select **Yes** to accept the EULA when prompted.
5. When prompted, enter a password for the `beacon` appliance user account, and then press **Enter**. You will be asked to enter the password twice.
6. When prompted, enter a password for the `admin` *web interface user account*.
7. Enter the requested SSL details to create a self-signed certificate and certificate signing request (CSR).

An **Installation Complete** dialog will confirm the completion of the appliance setup process. To *complete the configuration process*, access the web interface by navigating to `https://[APPLIANCE_ADDRESS]` in a supported browser.

Note

- To abort the setup script, press **Ctrl+C** or select **Cancel/No** at any time.The script and its auxilliary runmodes can be re-run from the CLI at a later time using the `beaconctl` *command set*.
- When multiple DNS servers are defined, they are queried in the order entered when resolving IP addresses.
- The self-signed certificate created during setup can later be replaced with a CA-signed certificate as described *here*.

4.1.4.2 Licensing and SSL

Upon logging in to the Endpoint Analytics web interface for the first time using the `admin` account, the user will be able to add a license key to activate the product. A CA-signed SSL certificate may also be installed to replace the previously created self-signed certificate at this point.

Adding a license key

An Endpoint Analytics license key can be obtained by contacting *Plixer Technical Support*. You will be asked to provide your appliance's unique machine ID, which can be found by navigating to **Configuration > Upload License Key** in the web interface.

Once acquired, paste the active license key into the field on the **Upload License Key** page, and then click **Upload Key**.

After a license key has successfully been uploaded, the **Upload License Key** page will display the following details for the currently applied license:

- Appliance hostname
- License type
- Expiration date

Note

The dashboard header in the web interface will display a warning message once the system detects that your license key is due to expire within 30 days.

Installing a CA-signed SSL certificate

As long as the system is set to use the self-signed SSL certificate created during the initial configuration process, browsers will return an untrusted certificate warning, which must be overridden to access the web interface.

To avoid this behavior, an SSL certificate that has been signed by an internal or commercial Certificate Authority (CA) will need to be installed:

1. Navigate to **Configuration > Manage Certificate**, click the **Download CSR** button, and then save the *Certificate Signing Request* to local storage.
2. Forward the CSR file to the CA for digital signing.
3. After receiving the Endpoint Analytics appliance certificate and the *CA Bundle* certificate in PEM format from the CA, copy the files to a location that can be accessed via the Endpoint Analytics web interface.
4. Return to the **Manage Certificate** page, and then click the **Choose File** button under SSL Certificate to browse to the appliance certificate file (.crt).
5. Still on the **Manage Certificate** page, click the **Choose File** button under CA Certificate to browse to the CA certificate file (.pem).

6. After both files have been selected, click **Upload Certificate Files**, and then wait for the confirmation that the files have been successfully uploaded.

To verify that the web interface is using the correct SSL certificate, use a browser to navigate to the login page using the FQDN specified in the CA-signed certificate. The browser should no longer return an untrusted certificate warning and the padlock icon in the address bar should be locked instead of open.

4.2 Configuration Guides

Endpoint Analytics ships with default settings that are suitable for common usage scenarios, but the system can also be further tuned to match the environment it will be deployed in.

After logging in with the `admin` web interface account, selecting **Configuration** from the navigation pane will display all available configuration submenus.

> **Important**
>
> Navigating away from any of the configuration pages without clicking on the *Save* button will cause any changes made to be discarded.

Subnet groups

Network subnet settings and IP address management for endpoint discovery and monitoring

Subnet groups **Data Processing**

Data processing settings and system performance parameters for optimal endpoint analytics operation

Data processing **Data Collection**

Data collection settings including SNMP, web user agents, RADIUS accounting, and ERSPAN traffic

Data collection **Active Directory Servers**

Microsoft Active Directory servers and LDAP settings for endpoint data collection from domain members

Active Directory servers **DNS Zones**

DNS server settings and hostname resolution options for endpoint identification and monitoring

DNS zones **Network Devices**

Switches, routers, and other infrastructure components for data collection

Network devices **Profiles**

Device profiles and classification rules for automatic endpoint categorization and policy assignment

Profiles **Events**

Event logging, alerts, and notification settings for system monitoring and security events

Events **Accounts**

User accounts, permissions, and authentication settings for system access and administration

Accounts

4.2.1 Subnet groups

Because Endpoint Analytics monitors all network traffic and NetFlow data forwarded to its monitoring interface(s), it is necessary to limit its collection functions to cover only endpoints of interest by specifying the networks or address spaces those endpoints are associated with.

The **Configuration > Subnet Groups** submenu of the web interface allows users to manage the subnet groups and address blocks whose network traffic and NetFlow data should be processed by the system.

> **Important**
>
> At least one subnet group with a valid address block must be added to the system before Endpoint Analytics can start collecting data.

4.2.1.1 Adding a subnet group

To add a new subnet group to the system, follow these steps:

1. Select the **Add Subnet Group** option from the **Subnet Groups** configuration submenu.
2. Enter a name for the subnet group, and then click **Continue**.
3. On the **Edit Subnet Group** page, click the **Add** button, and then enter the address block in CIDR format in the popup that opens.

> **Hint**
>
> To add multiple address blocks, use the **Add Multiple Address Blocks** button and enter one address block per line in the popup.

4. *(Optional)* To add an IP address space to exclude from the address block, click the **Add** (or *Add Multiple Address Blocks*) button under the **Exclude** section of the page. These buttons will be greyed out if an internal address block has yet to be added.
5. Under the **Listening Interfaces** section of the page, click the **Add New Interface** button, and then select an interface name from the dropdown in the popup that opens.
6. If needed, enter a filter as a tcpdump/lipcap style expression to define which packets should be accepted by the system before clicking the **Add** button to add the interface.

> **Note**
>
> If no filter is entered, all packets received via the selected interface will be accepted.

7. Enable NetFlow collection by clicking the **Edit NetFlow** button and ticking the checkbox in the popup that opens (this will also enable sFlow collection on port 6343 by default). If necessary, enter a new port for sFlow collection before clicking the **Save NetFlow** button.
8. Return to the top of the page, and save the subnet group configuration by clicking the **Save** button.

4.2.1.2 Editing subnet group settings

To modify the configuration of an existing subnet group, follow these steps:

1. Select the **List Subnet Groups** option from the **Subnet Groups** configuration submenu.
2. Click on the name of the subnet group to open the **Edit Subnet Group** page.

3. Make the necessary changes to the subnet group configuration.
4. Click the *Save* button to save the current configuration.

> **Note**
>
> The name of a subnet group cannot be edited. If a new subnet group name is needed, delete the existing subnet group and create a new one with the same configuration.

4.2.1.3 Deleting a subnet group

To permanently delete a subnet group from the system, follow these steps:

1. Select the **List Subnet Groups** option from the **Subnet Groups** configuration submenu.
2. Click on the name of the subnet group to open the **Edit Subnet Group** page.
3. Click the **Delete** button and read the warning in the confirmation popup.
4. Click **Yes** to confirm the deletion and return to the main subnet group list page.

4.2.2 Data processing

Endpoint Analytics' data processing settings control how the system collects, stores, and otherwise manages data globally. These settings can be configured by selecting **Data Processing** from the **Configuration** menu group in the web interface.

The **Configure Data Processing** page is divided into six sections:

4.2.2.1 Database maintenance

The settings under the **Database Maintenance** section of the data processing configuration page control if and how often the system purges the different types of endpoint data it collects. These can be used to automatically purge unused data from the system at regular intervals.

By default, most of the values will be set to 0, which means all endpoint data of those types will be retained by the system indefinitely.

The following table lists all of the settings under the **Database Maintenance** section:

Setting	Description	Unit	Default
Endpoint Timeout	Amount of time before an inactive endpoint is flagged as retired and removed from primary endpoint views (endpoint data will be purged, but historical data will be retained for the configured historical limit)	Days	0
Endpoint Removal	Amount of time before a retired endpoint and any retained data associated with it are permanently purged from the database	Days	0
Port Timeout	Amount of time before an endpoint whose location (switch/port) has not been updated has its location data removed	Hour	0
ARP Timeout	Amount of time before an endpoint whose IP-to-MAC has not been refreshed via any of Endpoint Analytics' collection mechanisms has its IP-to-MAC mapping data cleared from the database	Hour	0
Wireless Timeout	Amount of time before data for an endpoint that was discovered through a wireless access point will be retained without any updates to that data	Hour	0
Historical Limit	Amount of time that the system stores historical endpoint data (MAC history by port/IP/profile) for MAC-discovered endpoints, regardless of the endpoint's current state (active or retired)	Days	30
Event History	Amount of time that the system retains historical event data for an endpoint in the database	Mont	12
Custom Data Auto Removal	When toggled on, custom data objects are automatically deleted when the associated endpoint is removed from the system	N/A	Off

4.2.2.2 Network mapping

The following settings under the **Network Mapping** section of the data processing configuration page can be used to control how the system collects data using certain protocols or methods:

CDP Exclusion

List of *Cisco Discovery Protocol* (CDP) data strings that will be excluded from the system's default behavior of designating CDP-enabled NID ports as trunks

LLDP Exclusion

List of *Link Layer Discovery Protocol* (LLDP) data strings that will be excluded from the system's default behavior of designating ports on LLDP-enabled NIDs as trunks

> **Note**
>
> The CDP and LLDP exclusion lists can be updated via a local file (obtained from Plixer Support) or the CDN server (requires an Internet connection) using the buttons below each setting. The third button will revert them to the default exclusion lists stored on the appliance.

Trust Cisco MAC Notification Trap

If this checkbox is ticked, the system will accept endpoint data in Cisco and Enterasys MAC notification traps without initiating an SNMP poll for bridge MIB information upon receiving the trap (enabled by default)

Verify Cisco MAC Notification Trap

If this checkbox is ticked, the system will verify an endpoint's location information during subsequent polls after receiving a Cisco or Enterasys MAC notification trap (disabled by default)

> **Hint**
>
> When both enabled, the CISCO MAC notification trap settings can greatly reduce SNMP traffic on the network, but are only recommended when community string verification has been enabled for traps.

4.2.2.3 Active Directory

The **Active Directory** section of the data processing configuration page contains the following additional settings for collecting Active Directory data:

- **Ignore Disabled Computer Objects**: When this setting is enabled, all disabled AD computer objects are ignored when performing AD lookups. This setting is disabled by default.
- **Allow DNS for Active Directory Linking**: This setting enables the use of DNS hostnames (in addition to DHCP-derived hostname data) when performing AD computer object lookups. This setting is disabled by default.
- **AD DHCP Data Association Fade**: Indicates the number of days that the system will continue to use a DHCP hostname for AD lookups even when the DNS hostname data is more recent. The default value is set to 0, which means that the DHCP hostname will always be prioritized over DNS data, regardless of the former's age.
- **Hostname to MAC Address Association Limit**: Sets the number of MAC addresses that can be associated with a single hostname for endpoints that have multiple network interfaces. The default value is 2.

4.2.2.4 Advanced options

The **Advanced Options** section of the data processing configuration page contains additional settings for several of Endpoint Analytics' specialized features.

Instant Lookup

The *Instant Lookup* feature enables the system to perform on-the-fly DNS or Active Directory queries to collect supplemental information right as a client connects instead of relying on a polling cycle to capture data. Discovered endpoints will immediately trigger a DNS or AD lookup if there are no others in the queue. This results in improved speed and accuracy when assigning profiles to newly discovered endpoints.

This feature requires Endpoint Analytics to receive DHCP request packets (via a SPAN of DHCP server traffic or IP Helper configured on routers) and will initially rely on an endpoint's DHCP hostname to query DNS servers.

The following settings are used to configure *Instant Lookup*:

- **Active Directory Query Queue** - Sets the amount of time that an endpoint will wait in queue before being released for AD Instant Lookup (default: 15 seconds)
- **DNS Query Queue** - Sets the amount of time that an endpoint will wait in queue before being released for DNS Instant Lookup (default: 15 seconds)
- **DHCP Client Vendor Inclusion** - List of DHCP client vendors (in regular expressions) whose endpoints will be subject to Instant Lookup (click the *Default DHCP Client Vendor Inclusion List* button to revert to the default list)
- **Bypass DHCP Client Vendor Inclusion List** - Enables DNS-based Instant Lookup for all client vendors (disabled by default)

4.2.2.5 Miscellaneous

The **Miscellaneous** section of the data processing configuration page contains additional settings that control how Endpoint Analytics collects and/or processes data in specific scenarios.

Ignore PXE

Ticking this checkbox will instruct the Endpoint Profiling Engine to discard all PXE-related traffic and can significantly reduce database processing and storage overhead in environments that boot from remote images over the network.

4.2.2.6 Re-mapping and re-modeling

It is not necessary to restart the Endpoint Analytics appliance for most changes to the system configuration to take effect after they are saved. Instead, the system functions affected by the changes can be re-initiated manually using the buttons on the **Configure Data Processing** page.

Re-map

Instructs the system to immediately poll all NIDs and update the network topology map maintained in the database

Re-model

Instructs the system to re-evaluate and reassign profiles to all endpoints based on the current information in the database

Individual endpoints are modeled automatically upon discovery, but a full re-model is required when new *profiles* or *events* are added/removed or enabled/disabled.

When either button is clicked, a message confirming that the process has been initiated will be displayed. Re-mapping and re-modeling may take several minutes for very large systems, large databases, and/or complex configurations, and it is normal for resource usage on the appliance to peak during the process.

4.2.3 Data collection

Endpoint Analytics relies on several software modules to collect endpoint data, and certain parameters of their functions can be configured by navigating to **Configuration > Data Collection**.

The **Configure Data Collection** page allows the user to modify the following settings:

SNMP Trap Collection Community String
: Sets the community string that NIDs must be configured to send with their link state and MAC change traps

Web User Agent Collection Filter
: Instructs the system to exclude web user agents that contain the specified string(s) from data collection (strings must be concatenated within a single regular expression using the | operator)

> **Hint**
>
> Adding a web user agent collection filter will not clear existing data from the database. To purge collected web user agent data from the system, use the *Cleanup Database* button on the **System Summary** page under the Utilities menu group.

Enable RADIUS Accounting Collection
: Ticking this checkbox will allow the system to receive and process RADIUS accounting data from RADIUS clients (must be added via the *Add Device* page under **Configuration > Network Devices**)

RADIUS Accounting Port
: Specifies the port number on which RADIUS clients export their account data when RADIUS accounting collection is enabled (default: 1813)

RADIUS Accounting Forwarding
: In scenarios where a RADIUS client, such as an access switch, is only capable of sending RADIUS accounting data to a single recipient, Endpoint Analytics can also be configured to forward the data to one or more upstream RADIUS servers based on a priority list.

To add an upstream server to the system's list of RADIUS accounting forwarding recipients, follow these steps:

1. Click the **Add RADIUS Accounting Forwarding** button (RADIUS accounting collection must be enabled first).
2. Under **Proxy**, enter the IP address of the RADIUS proxy server to forward the data to.
3. Under **Port**, enter the port number the proxy server will be listening on.
4. Enter the shared secret that the proxy server will be expecting to see.
5. Click the **Save** button to save the RADIUS proxy server configuration.

After receiving data from the client, Endpoint Analytics will forward the packets to each of the configured upstream servers in turn until it receives a response or the list is exhausted. Once a response is received, it will be sent to the downstream RADIUS client.

The up and down arrows can be used to adjust the priority ranking of upstream RADIUS servers in the list.

> **Note**
>
> Endpoint Analytics will wait 90 seconds for a response before abandoning forwarded packets and attempting to contact the next upstream server in the list.

4.2.3.1 ERSPAN Configuration

Endpoint Analytics can be configured to receive ERSPAN traffic from CISCO devices supporting the feature.

To set up a monitoring interface for ERSPAN packets, enter the following details in the fields provided:

- Interface to use (must be *added to the virtual appliance* first)
- A name to identify the ERSPAN virtual interface by in Endpoint Analytics functions
- Source IP address of ERSPAN traffic
- Destination IP address (to be connected to the selected interface)
- Destination IP address subnet mask/CIDR (number only)
- ERSPAN ID/key (must match ID configured on the source device)

> **Note**
>
> After adding, modifying, or removing an ERSPAN configuration, the system will perform a *re-map and re-model* to apply the necessary changes.

4.2.4 Active Directory servers

Endpoint Analytics treats Microsoft Active Directory as a "trusted" source of information when collecting endpoint data from members of an AD domain. Because data is collected by querying AD domain controllers using LDAP, the system must be configured with both the AD server information and the credentials of a user with LDAP query privileges. The Base DN from which to begin the query is also required.

AD server settings can be configured by navigating to **Configuration** > **Active Directory Servers**.

4.2.4.1 Adding an Active Directory Server

To configure a new AD server, select **Add Active Directory Server** from the AD server configuration submenu, and then follow these steps:

1. Under **Server Name:**, enter the server name in FQDN format (required if LDAPS is enabled) or the server IP address.
2. If the *Use LDAPS* checkbox is ticked, an additional field labeled *Certificate (PEM Format)* will be displayed. Paste the PEM-formatted CA certificate chain into this field or use the *Upload Certificate* button to upload it from a local file.
3. Under **Description:**, enter an optional description for the current AD server record.
4. Under **User Name:**, enter the user name for an AD service account with the required access privileges (LDAP or LDAPS) using the format `username@ad.domain.com`.
5. Under **Password:**, enter the current password for the AD service account.
6. Under **Base DN:**, enter the Base DN for the LDAP/LDAPS lookup. Click the **Suggest Base DN** button to have the system pull the Base DN from the domain name of the service account.
7. If desired, click the **Test Connection** button to verify the details entered. Click the **Save** button to save the configuration when done.

Multiple AD servers can be added by repeating these steps. Servers can also be added using the *Add Active Directory Server* button on the Active Directory servers list page.

Once added, an Active Directory server will be queried by the system every 120 minutes.

4.2.4.2 Editing/deleting an Active Directory server

To delete or modify an existing Active Directory server from the system, follow these steps:

1. Select **List Active Directory Servers** from the **Active Directory Servers** configuration submenu.
2. Click on any AD server name to open the **Edit Active Directory Server** page.
3. From there, you can either edit the configured settings or click the **Delete** button to delete the server.
4. Click **Save**.

> **Hint**
>
> For larger AD deployments (over 2,500 computer objects per DC), it may be ideal to configure multiple AD server instances for a single physical AD server within Endpoint Analytics, so that LDAP queries for computer objects can be initiated from two more Base DNs.

4.2.5 DNS zones

> **Important**
>
> Ensure that DNS Zone Transfers are allowed and enabled on the DNS server for the Endpoint Analytics IP address.

The **Configuration > DNS Zones** submenu contains several options for DNS zone configuration and management:

4.2.5.1 Adding a new DNS zone

To configure a new DNS zone, select *Add DNS Zone* from the **DNS Zones** configuration submenu and follow these steps:

1. Under **DNS Zone:**, enter a name for the DNS zone to be added.
2. Under **DNS Server:**, enter the FQDN or IP address of the DNS server to be queried for the zone.
3. Tick the **Enable DNS Zone** checkbox to enable the zone once it is added.
4. *(Optional)* If TSIG authentication is required for the DNS zone/server, select the key type from the drop down under **TSIG**, and then enter the unique key name and the key value provided by your DNS administrator in the fields under **Key Name:** and **Key Value:**, respectively.
5. If desired, click the **Test Connection** button to verify the details entered, and then click **Save**.

New DNS zones can also be added from the DNS zone list via the **Add DNS Zone** button.

4.2.5.2 Editing/deleting a DNS zone

To delete or modify an existing DNS zone from the system, follow these steps:

1. Select **List DNS Zones** from the **DNS Zones** configuration submenu.
2. Click on any DNS zone name to open its **Edit DNS Zone** page.
3. From there, you can either edit the configured settings or click the **Delete** button to delete the DNS zone.
4. Click **Save**.

4.2.5.3 Adding multiple DNS zones

To add multiple DNS zones from a CSV file, follow these steps:

1. Select **Import DNS Zones** from the **DNS Zones** configuration submenu or click on the button on the DNS zones list page.
2. Click the **Choose File** button, and then browse to the CSV file.

Important

The file should contain a name, DNS server FQDN or IP address, and TSIG details (if required) for each DNS zone to be added. CSV file templates can be downloaded from the **Import DNS Zones** page (use the *No Keys* template when TSIG authentication is not required).

3. After selecting the CSV file, click **Import File**.
4. Verify that the zone details are correct and complete. Entries can also be omitted or added in a disabled state from the popup. Click the **Import DNS Zones** button when done.

4.2.6 Network devices

Before Endpoint Analytics can start collecting endpoint data from network interface devices (NIDs), they will first need to be added to the system using the **Configuration > Network Devices** submenu.

Note

Endpoint Analytics can collect endpoint information from switches and routers using SNMP versions 1, 2c, and 3. The system will poll devices using either the SNMP version set in the individual device configurations or the

version set for the network device group (if the device has been assigned to one). Devices configured for SNMP v1 will **not** respond to v2c queries.

The options under the submenu correspond to the following network device management tasks:

4.2.6.1 Adding a network device

To configure a new network device, select **Add Device** under **Configuration > Network Devices**, and then do the following:

1. In the **Name** section of the **Add Network Device** page, enter a unique, case-sensitive name to identify the device and the IP address that it uses for SNMP queries.
2. (Optional) To add the device to an existing network device group, select the group name from the dropdown menu.
3. In the **Access** section of the page, select the SNMP version to use for communication with the device, and then enter the read-only community string. The community string is required for SNMP v1 and v2c.

Note

When a network device is assigned to a device group, the group's SNMP version and community string settings will override its individual device settings.

3a. If SNMPv3 is selected as the communication method, then the following settings will also need to be configured:

- User Name - Used to authenticate an SNMPv3 session with the device.
- Security Level - Enables or disables hashing and/or encryption.
- Hash Type - Hash function that is used by the device (SHA1 or MD5, only available for *AuthNoPriv* and *AuthPriv* security levels).
- Authentication Passphrase - Passphrase that is used with the selected hash type.
- Encryption Type - Encryption type that is used by the device (AES128 or DES, only available with *AuthPriv* security level).
- Privacy Passphrase - Passphrase that is used with the selected encryption type.

4. Select **Poll as Endpoint** to allow Endpoint Analytics to treat the device as an endpoint rather than a network device. If the device does not support MAC notification traps (i.e. not a Cisco or Enterasys device or has MAC notification traps disabled), then select **Does not support MAC notification traps**.
5. (Optional) In the **RADIUS** section of the page, select **Enable RADIUS** to allow the system to process RADIUS accounting data from the device, and then enter the Shared Secret set on the device.
6. (Optional) In **Trunk Ports**, select **Edit All** to manually designate ports as trunk ports. This process is used when the system is unable to automatically identify trunk ports using CDP or by inspecting the SAT of the device. Port numbers can be entered as individual comma-separated numbers or port ranges (e.g., "1-5").

Hint

Designating a port as a trunk does not disable endpoint discovery on that port, but it instructs the UI not to display the MAC addresses learned on that port when viewing endpoints by network device port.

7. (Optional) In **Ignored Trunk Ports**, click **Edit All** to add known trunk ports to be treated as regular switch ports so that the UI displays the MAC addresses learned on those ports.
8. Click **Save** to save the configuration and establish SNMP communication with the network device.

4.2.6.2 Adding a network device group

Device groups allow certain settings to be applied **over** the individual configurations of devices assigned to them and can be used to streamline device administration and management in larger network environments.

> **Note**
>
> The settings configured for the group are automatically applied to all new devices added to the device group. The original configurations of these devices are overwritten.

To add a new network device group, select **Add Group** under **Configuration > Network Devices**, and then do the following:

1. In the **Name** section of the **Add Network Device Group** page, enter a unique, case-sensitive name for the device group.
2. In the **Access** section of the page, select the SNMP version to use to communicate with **all** devices in this group, and then enter the read-only community string that the devices have been configured with. The community string is required for SNMP v1 and v2c.

   2a. If SNMPv3 is selected as the communication method for the group, then the following settings will also need to be configured:

   - **User Name** - Used to authenticate SNMPv3 sessions with the devices in the group.
   - **Security Level** - Enables or disables hashing and/or encryption for devices in the group.
   - **Hash Type** - Hash function that is used by the devices in the group (SHA1 or MD5, only available for *AuthNoPriv* and *AuthPriv* security levels).
   - **Authentication Passphrase** - Passphrase that is used by the devices in the group with the selected hash type.
   - **Encryption Type** - Encryption type that is used by the devices in the group (AES128 or DES, only available with *AuthPriv* security level).
   - **Privacy Passphrase** - Passphrase that is used by the devices in the group with the selected encryption type.
3. Select **Poll as Endpoint** to allow Endpoint Analytics to treat the devices in this group as endpoints rather than network devices. If none of the devices in the group support MAC notification traps (i.e. not Cisco or Enterasys devices or have MAC notification traps disabled), then select **Does not support MAC notification traps**.
4. (Optional) In the **RADIUS** section of the page, select **Enable RADIUS** to allow the system to process RADIUS accounting data from devices in this group, and then enter the shared secret set on the physical devices.
5. Click **Save** to save the device group configuration.

4.2.6.3 Device and group management

The *List Devices*, *List Groups*, and *Unconfigured Devices* options under **Configuration > Network Devices** serve as the main administrative console for network devices and device groups once an initial batch of devices and groups has been configured.

Each menu item provides access to the tools and functionality necessary for the efficient management of the corresponding entities.

Network device management

Selecting **List Devices** from the **Network Devices** configuration submenu opens a summary page that lists all the network devices that have been added to the system.

> **Note**
>
> To apply a filter to the device list, enter text in the *Name/Description* and/or *IP Address* fields or click one of the device counts in the page header.

The following device management operations can also be accessed from the *List Devices* page:

Adding a new device

Clicking **Add Device** opens the **Add Network Device** page. The **Add Network Device** page can also be accessed by clicking *Add Device* in the **Network Devices** configuration submenu.

Editing device settings

Clicking the IP address of a network device in the list opens its **Edit Network Device** page where the current device settings can be modified.

The following settings/options are only available in the **Edit Network Device** page:

- **Context** - Clicking **Add** opens a popup window to attach SNMP context information to the device. This setting is disabled if *Poll as Endpoint* is selected.
- **Translated Addresses** - Clicking *Add* opens a popup window to attach the additional IP addresses that will be polled on the physical device.
- **Device Ports** - Opens a list of physical ports and connected endpoints. This setting can also be accessed by navigating to **Endpoints > By Network Device > Ports**.
- **Clear Device Ports** - Removes current endpoint information from all ports.
- **Query Now** - Triggers an immediate SNMP poll of the network device.

Deleting network devices

Network devices can be deleted individually through its **Edit Network Device** page. Multiple network devices can be deleted at once by selecting multiple devices, and then clicking **Delete Selected Devices**.

Adding a network device to a group

A network device can be added (or reassigned) to a device group through its **Edit Network Device** page, and then selecting a device group from the dropdown menu.

Exporting device information

Clicking **Export as** exports the device information as a CSV file. A smaller subset of the list can also be exported by selecting multiple endpoints before clicking on the CSV export button.

Device group management

Selecting **List Groups** in the **Network Devices** submenu opens a summary page that lists all the configured network device groups. The list also includes an *Ungrouped* category that contains all ungrouped devices.

Clicking the + button next to a group name expands the group and displays all the NIDs assigned to it.

Expanding a group allows the following actions to be performed:

Adding a device group

Clicking **Add Device Group** opens the **Add Network Device Group** page. The **Add Network Device Group** page can also be accessed by clicking **Add Group** in the **Network Devices** configuration submenu.

Editing device group settings

Clicking the name of a device group opens its **Edit Network Device Group** page where the current group settings can be modified.

Editing device settings

Clicking the name of a network device opens its **Edit Network Device** page. For more details on this page, see *network device management*.

Changing group assignments

One or more NIDs can be assigned to a different group by selecting the new group from the dropdown menu, and then clicking **Change Group**.

Clicking **Ungroup Selected** removes the selected devices from the current group without assigning them to a new group.

Removing devices from the system

Select one or more NIDs, and then click **Remove Selected** to permanently delete the devices from the system.

Clicking **Remove ALL Network Infrastructure Devices** permanently deletes all NIDs in the group from the system.

Unconfigured devices

Selecting **Unconfigured Devices** in the **Network Devices** configuration submenu opens a summary page that lists all network devices that have been discovered but are not configured as network devices under the Endpoint Analytics environment.

> **Hint**
>
> This view may also include network devices that have multiple IP addresses associated with their SNMP agent. The additional interfaces will need to be mapped to their main network device, if it has already been configured in the system.

The **Unconfigured Devices** page displays the information that is extracted from the CDP or LLDP data of each unconfigured device. The following details are shown for the discovered devices:

- **Name** - Name that is configured in the device
- **IP Address** - IP address of the primary interface of the device
- **System Description** - Current value of the SysDescr OID on the device (including the full name and version identifier of the system hardware), its OS, and its networking software
- **Known Name Found** - Indicates whether the device name matches the name of a network device that has already been configured in the system
- **Updated** - Timestamp of the most recent data captured from the device. Clicking the refresh button shows the latest device data

The following actions can also be performed:

Adding a device

Clicking **Add** opens the **Add Network Device** page with fields that are pre-populated with the discovered information.

Mapping a device

Clicking **Map** maps the device data to an already configured network device by adding its IP address as a secondary interface (under **Translated Addresses**).

> **Note**
>
> Devices that have been added or mapped will be not be listed in the **Unconfigured Devices** page.

Exporting device information

The contents of the **Unconfigured Devices** page can be exported as a CSV file by clicking the corresponding **Export as** button.

4.2.6.4 Importing network device and group information

NIDs and device groups can also be added in batches by selecting either *Import Devices* or *Import Groups* from the **Network Devices** configuration submenu.

Importing devices

To add multiple network devices as a batch, select the *Import Devices* option, and then do the following in the **Import Network Devices** page:

1. Download the CSV file template that corresponds to the SNMP version for the devices to be added (SNMPV1-2C or SNMPV3), and then populate the columns with the necessary device details. For additional information, see *adding a network device*.
2. Click **Choose File**, browse to the edited CSV file, and then click **Import File**.
3. In the **Import Network Device Information** form, select the correct SNMP version for the devices to be added, and then if necessary, select **Poll as Endpoint**.

> **Hint**
>
> Use the *Omit* checkboxes and *Edit* button in the form to make any necessary changes to the data before importing it. An error message is also displayed when duplicate IP addresses are found.

4. Verify that the details are correct and complete, and then click **Import Devices** to add the devices to the system.

Importing device groups

To add multiple device groups as a batch, select **Import Groups**, and then do the following in the **Import Network Device Groups** page:

1. Download the CSV file template that corresponds to the SNMP version for the device groups to be added (SNMPV1-2C or SNMPV3), and then populate the columns with the necessary group details. For additional information, see *adding a network device group*.
2. Click **Choose File**, browse to the edited CSV file, and then click **Import File**.

3. In the **Import Network Device Group Information** form, select the correct SNMP version for the device groups to be added, and then, if necessary, select **Poll as Endpoint**.

> **Hint**
>
> Use the *Omit* checkboxes and *Edit* button in the form to make any necessary changes to the data before importing it.

4. Verify that the details are correct and complete, and then click **Import Device Groups** to add the groups to the system.

4.2.6.5 Data collection matrix

The following tables show the different collection methods and data types used by Endpoint Analytics to configure your devices and/or firewalls.

Collection methods

Collection Method	Function	Notes
		Discovery
SNMP Polling	MAC-identity ••• IP-identity •• Location •••	Identifying Attributes ••
SNMP Traps	MAC-identity •• Location •• Real-Time ••	
SPAN DHCP	MAC-identity •• IP-identity •• Real-Time •	Identifying Attributes •• Operating System ••
SPAN Other	MAC-identity • IP-identity •	Identifying Attributes •••/•• Behavioral Attributes •• Operating System ••
IP Helper	MAC-identity •• Real-Time •	Identifying Attributes •• Operating System ••
Active Directory Queries		Identifying Attributes •• Operating System ••
RADIUS Accounting	MAC-identity •• IP-identity •• Location •• Real-Time ••	Behavioral Attributes ••
NetFlow, J-Flow, SFlow		Identifying Attributes • Behavioral Attributes •
DNS Transfers		Identifying Attributes •

Classification:

- Required: •••
- Recommended: ••
- Supplemental: •

Data types

The *SPAN* column in the following table indicates whether the data type is collected through receiving SPAN traffic.

SPA	Data Type	Functionality	Configuration
No	Active Directory	Profile data (computer info, OS, SP, etc.)	Active directory collection (EA)
No	DHCP Request Data	Profile data (vendor, hostname, request options, other options), informative (FQDN), logistics (location), initial discovery	IP helper (external), subnet groups (EA)
No	DNS Names	Informative (IP to DNS mapping)	Zone transfers, DNS zones (EA)
No	CDP/LLDP	Initial discovery, logistics (trunk ports, port status, authentication status, location), profile data	SNMP collection (EA)
No	IP - ARP Cache	Mac to IP binding	SNMP collection (EA)
No	IP - RADIUS	Mac to IP binding, logistics (location)	RADIUS accounting forwarding (external)
No	MAC - SNMP Traps	Initial discovery	SNMP trap forwarding (external)
No	MAC - ARP Cache/SNMP General	Initial discovery, profile data, logistics (location)	SNMP collection (EA)
No	Location - Other	Logistics (location)	Internal algorithm, UI
No	RADIUS Usernames	Informative (radius usernames to MAC)	RADIUS accounting forwarding (external)
No	SNMP Description	Profile data	SNMP collection (EA)
No	Traffic - NetRelay	Profile data	Flow forwarding (external)
Yes	DICOM/Healthcare	Profile data	SPAN (external)
Yes	IP - ARP Transaction	MAC to IP binding	SPAN (external)
Yes	IP - DHCP Response	MAC to IP binding	SPAN (external)
Yes	MAC - Traffic	Initial discovery, profile data	SPAN (external)
Yes	Stack Info	Profile data (TTL, window size, TCP options)	SPAN (external)
Yes	Network Traffic	Profile data (ports), informative (connections)	SPAN (external)
Yes	URL	Profile data	SPAN (external)
Yes	Web User Agent	Profile data	SPAN (external)

> **Note**
>
> NetWatch will still observe local traffic without SPAN.

4.2.7 Profiles

Endpoint Analytics ships with an extensive library of preconfigured *endpoint profiles* and profile groups as part of its software. Profile and profile group configurations are all factory defined, but certain options controlling their use are user-configurable.

The **Configuration > Profiles** submenu provides access to the following profile management actions:

4.2.7.1 Enabling/disabling profiles

There are several ways to enable and disable profiles, as well as to access their other user-facing options from the **Profiles** configuration submenu:

Edit profile page

To open the **Edit Profile** page for a profile, select **List Profiles**, and then click on the profile name. This page will display additional details about the profile and list the profile rules governing its assignment to endpoints.

This page also provides access to the following options:

- *Profile Enabled* - Ticking this checkbox will enable the profile for use by the system (enabled by default)
- *Allow Timeouts* - Ticking this checkbox will apply the timeout settings configured under **Configuration > Data Processing** to the endpoints in this group and the data collected from them

List profiles page

To enable/disable and toggle timeout for multiple profiles, select them using the checkboxes on the **List Profiles** page, and then click the **Modify Selected** button at the bottom of the page.

This will open a popup with *Profile Enabled* and *Timeout* checkboxes for the selected profiles. The settings can also be applied to all profiles listed in the popup using the corresponding *Set All* checkboxes, and the *Reset* button can be used to revert the settings for the selected profiles to their default state.

After modifying the settings for the profiles, click the **Save Changes** button to save the configuration and close the popup.

4.2.7.2 Profile management

The **Manage Profiles** page allows certain batch operations involving profiles to be performed without having to go through the **Edit Profile** page or manually selecting multiple profiles from the profile list page.

Enabling profiles

To enable a group of profiles from the **Manage Profiles** page, follow these steps:

1. Tick the **Enable Profiles** radio button at the top of the page.
2. Select the initial subset of profiles to enable from the dropdown menu (all, device, or OS).
3. Tick either the **All Profiles** radio button to perform the operation for all profiles in that subset or the **Certain Profile Groups** radio button to select profile groups to enable.
4. If enabling only certain profile groups, tick the checkboxes to select the profile groups to enable in the table that opens. Afterwards/otherwise, click the **Enable** button to complete the process.

Disabling profiles

To disable a group of profiles from the **Manage Profiles** page, follow these steps:

1. Tick the **Disable Profiles** radio button at the top of the page.
2. Select an action to perform from the dropdown menu (all, unused profiles, non-top matched profiles).
3. If *Disable All* was selected, select an initial subset of profiles to disable from the second dropdown menu (all, device, or OS).
4. Tick either the **All Profiles** radio button to perform the operation for all profiles in that subset or the **Certain Profile Groups** radio button to select profile groups to disable.
5. If disabling only certain profile groups, tick the checkboxes to select the profile groups to disable in the table that opens. Afterwards/otherwise, click the **Disable** button to complete the process.

Uploading an optimization file

As an alternative to other profile management methods, the **Manage Profiles** page allows an XML file containing the desired enabled/disabled and timeout allow values to be uploaded to the system. For the required file format/template, contact *Plixer Technical Support*.

To load the file and apply the provided values from the **Manage Profiles** page, follow these steps:

1. Tick the **Upload Optimization File** radio button at the top of the page.
2. Click the **Choose File** button, and then browse to the XML file.
3. Click the **Upload File** button to load the file.

4.2.7.3 Updating profile information

Endpoint Analytics' profile definitions are regularly updated with additional data, such as new MAC vendor information and the latest device details.

To update the current profile definitions, follow these steps:

1. Navigate to **Configuration > Profiles**, and then select **Update Profiles**.
2. Click the **Update from Website** button to view a changelog between the current and latest versions of the profile definitions.

> **Note**
>
> If the appliance is not able to access the internet, contact *Plixer Technical Support* to obtain the latest update file.

3. (Optional) Tick the **Override Enabled Status** checkbox to overwrite the current status of all profiles with the default values from the import file.
4. Click the **Update Profiles** button to continue and complete the update process.

After a profile update, it is recommended to *re-model the system* so that profiles can be reassigned to endpoints based on the latest definitions.

4.2.8 Events

Once an endpoint has been discovered and is being monitored, certain changes in its state or behavior will be logged by Endpoint Analytics as events, which can also be used to alert network and security operations.

By default, events will be delivered to the web interface and can be viewed in the *Recent Events* dashboard widget or the **View Endpoint Events** page under the *Endpoints menu group*, but they can also be configured for delivery to internal or external syslog servers.

The **Configuration > Events** submenu allows events to be configured to suit a wide range of usage scenarios.

4.2.8.1 Event types

Endpoint Analytics events can be configured as one of the following types:

New endpoint

Triggered when a new endpoint is initially discovered and/or when a profile is assigned to it (including not profiled).

> **Note**
>
> A factory-default *All New Endpoints* event is pre-configured to match all endpoint profiles and will be triggered whenever Endpoint Analytics discovers a new endpoint MAC address.

Profile change (entering)

Triggered when an endpoint is migrated from one profile assignment *to* the specified profile(s) (other than not profiled), such as when newly observed identity attributes observed result in a higher profile match score with a different profile.

Profile change (exiting)

Triggered when an endpoint is migrated *from* the specified profile(s) assignment to another or when an endpoint returns to being classified as *Not Profiled*.

Alarm profile

Triggered by user-defined *Alarm Profiles* that contain profile rules or MAC vendor information that may indicate the presence of endpoints with irregular, suspicious, or potentially dangerous attributes.

Profile consistency

Triggered when an endpoint in the specified profile(s) has identity attributes that satisfies the requirements of multiple profile assignments.

4.2.8.2 Adding events

To add a new event to the system, select **Add Event** from the events configuration submenu, and then do the following:

1. In *Event Name:*, enter a unique, case-sensitive name for the event.
2. (Optional) In *Event Logic:*, enter a regular expression that must be matched for a profile to be monitored for the event. If `/.*/` or no event logic expression is entered, then the event will trigger endpoints in any profile.

> **Note**
>
> In the case of alarm profile events, the event logic expression defines the alarm profile whose rules must be matched by endpoints to trigger the event.

3. Select the event type to be created from the dropdown menu. If it is a profile change event, select whether it is an entering or exiting event from the second dropdown menu.

4. (Optional) Select the checkbox under *Event Delivery Method:* to enable syslog delivery for the event. For additional information on configuring event delivery outside the web interface, see *delivering events to syslog*.
5. In *Event Level:*, select a severity level to assign to the event (used in various web interface views).
6. Enable the event, and then click **Save** to save the configuration.

> **Hint**
>
> The **Add Event** page can also be accessed by selecting **List Events** from the events configuration submenu, and then clicking **Add Event**.

Events are triggered only if they are enabled, and newly configured events are activated only after the next system re-model.

4.2.8.3 Delivering events to syslog

Endpoint Analytics events can be delivered to the internal system syslog or to external syslog servers for additional analysis after the necessary system-level changes are made through the appliance's OS.

> **Hint**
>
> If necessary, contact your system administrator or *Plixer Technical Support* for assistance with configuring these settings.

Event delivery to internal syslog

To configure the system for event delivery to internal syslog, do the following:

1. Open an SSH session to the Endpoint Analytics appliance, and then elevate to root with the `su` command.
2. Open the internal syslog configuration file by entering:

   ```
   # vi /etc/rsyslog.d/50-default.conf
   ```

3. In line 9 of the file, replace:

   ```
   *.*;auth,authpriv.none -/var/log/auth.log
   ```

   with:

   ```
   *.*;auth,authpriv.* -/var/log/auth.log
   ```

4. After saving the changes, enter the following command to restart the rsyslog service to apply the delivery changes:

   ```
   # systemctl restart rsyslog
   ```

With this configuration set, any events that have syslog delivery enabled will be logged to the internal syslog on the Endpoint Analytics appliance every time they are triggered.

Event delivery to external syslog

To configure the system for event delivery to an external syslog server, do the following:

1. Open an SSH session to the Endpoint Analytics appliance, and then elevate to root with the `su` command.
2. Open the internal syslog configuration file by entering:

```
# vi /etc/rsyslog.d/99-beacon.conf
```

3. In line 13 of the file, replace:

```
# authpriv.alert @log.host.port
```

   with:

```
# authpriv.alert @75.76.75.76:9992
```

   and replace 75.76.75.76:9992 with the syslog host address and listening port number.

4. After saving the changes, enter the following command to restart the rsyslog service to apply the delivery changes:

```
# systemctl restart rsyslog
```

With this configuration set, any events that have syslog delivery enabled will be logged to the external syslog server every time they are triggered.

syslog event format

syslog messages for Endpoint Analytics events are logged in the following format:

```
<EVENT_DATE_TIME> <SERVER_HOST_NAME> [<SYSLOG_PROCESS_ID>]:
<EVENT_TYPE>. Event Name: [<EVENT_NAME>] Switch/port:
<SWITCH_IP_ADDRESS>(<SWITCH_PORT_INDEX>) Profile: (<CURRENT_PROFILE>)
MAC: (<ENDPOINT_MAC_ADDRESS>) Old Profile: (<PREVIOUS_PROFILE>) End
node: <ENDPOINT_MAC_ADDRESS>(<ENDPOINT_IP_ADDRESS>)
```

4.2.8.4 Managing events

Selecting **List Events** from the events configuration submenu opens a summary page that lists all the configured events and their current settings in a table.

From the *Events List* page, the following event management actions can be performed:

Adding a new event

As an alternative to using the *Add Event* option under the events configuration submenu, click **Add Event** at the bottom of the table to open the **Add Event** page.

Inspecting or editing event settings

To view or edit the current settings of an event, click the event name in the list to open the **Edit Event** page. Events can also be enabled or disabled from this page.

Deleting an event

To delete an event, click the event name to open its **Edit Event** page, and then click **Delete** on the upper part of the page.

4.2.9 Accounts

Endpoint Analytics uses two types of accounts to control access to the system and its functions. In addition to the appliance-level `root` and `beacon` accounts configured during the deployment process, there are also user accounts that are exclusively tied to the web interface.

Account administration tasks for web interface user accounts are primarily handled via the **Configuration > Accounts** submenu.

4.2.9.1 Web interface account roles

User accounts fall under one of three roles within the web interface:

Administrator

The administrator is the highest privileged role within the web interface and can make configuration changes, in addition to being able to view all system data.

Only one administrator account exists per system, and it is primarily used for initial access to the web interface after deployment as well as managing other user accounts.

> **Note**
>
> Only one administrator account session is permitted from a given IP address.

Operator

Operator accounts have full access to the web interface and can make configuration changes, but they cannot change the user account settings.

Analyst

Apart from *customizing their dashboard page*, Analyst accounts have access to most Endpoint Analytics data pages and utilities, but they cannot view or modify the system configuration.

> **Hint**
>
> There is no limit to the number of Operator and Analyst accounts that can be created.

The password for the administrator web interface account can be changed by logging into the Endpoint Analytics appliance as the `beacon` user and running the following command:

```
# sudo /usr/beacon/www/bin/userAdmin.php -u 1 password <new_password>
```

> **Note**
>
> By default, all web interface sessions will automatically time out after being idle for 30 minutes. The idle timers cannot be disabled, but they can be adjusted between 5, 15, and 30 minutes for operator and analyst accounts.

4.2.9.2 Adding a new user

To add a new web interface user or account, select **Add Account** from the **Accounts** configuration submenu, and then do the following:

1. Under *Username:*, enter a unique username for the new user. The following characters cannot be used in usernames (or passwords): ;'|"()[]{}``
2. Under *Password:*, enter a password for the account, and then retype the password in the next field for verification.
3. Under *Access Level:*, select the *role* for the account. *Operator* is selected by default.
4. Under *Timezone Region:* and *Select Timezone:*, select a region and timezone for the user.
5. Under *Timeout:*, select the number of minutes a session must be idle before the account is automatically logged out.
6. Under *Enabled:*, select whether to enable the account once it is created.
7. After verifying that all details are correct, click **Save** to create the account.

> **Hint**
>
> The password, region, and timezone can be changed by the user by clicking the user menu button in the web interface banner and then selecting **My Settings** once the user is logged in.

New accounts can also be created by navigating to **Configuration > List Accounts**, and then clicking **Add Account** on the *summary page*.

4.2.9.3 Managing user accounts

Selecting **List Accounts** from the **Accounts** configuration submenu opens a summary page that lists all existing web interface accounts.

The **Accounts** list page displays the current settings for each configured user account and functions as the main hub for the following account management tasks:

Adding a new user or account

As an alternative to using the **Add Account** option under the Accounts configuration submenu, click **Add Account** at the bottom of the table to open the **Add Account** page.

Editing account settings

To edit the details of an account, click the username in the list to open the **Edit Account** page, and then make the necessary changes.

The following actions can also be performed from the **Edit Account** page:

- Resetting or changing the account password
- Enabling or disabling the account
- Deleting the account

4.2.9.4 Single Sign-On (SSO)

By default, the web server hosting the web interface handles all user authentication functions locally. As an alternative, Endpoint Analytics supports SSO authentication through third-party services.

> **Note**
>
> Only the operator and analyst accounts can be routed through third-party authentication services. The administrator account is always authenticated locally to make sure that it has permanent access to the system.

For additional information and instructions on configuring third-party identity providers, see the *subsection on SSO integration*.

4.2.9.5 Audit Logging

Endpoint Analytics can log UI activity either locally (to `/var/log/audit.log`) or to an external syslog server. UI audit logging is disabled by default.

> **Note**
>
> UI audit log messages delivered to `/var/log/audit.log` require root privileges to view using the `tail`, `cat`, `more`, or `less` commands.

To enable audit logging, rename the `audit.xml.sample` file found in `/usr/beacon/config` to `audit.xml`, and then edit it to set the desired level of audit logging. The default configuration of the file is for full UI audit logging with delivery to the internal syslog.

Audit log message formats

Endpoint Analytics supports five audit logging formats for output to internal or external syslog. The following audit logging formats can be enabled by setting their respective rule values to true in the `audit.xml` file:

- **page** - Basic format used for auditing page access.

```
<rule name="page" type="boolean" default="false" value="true"/>
```

- **rpc** - Format used for auditing all json-rpc methods.

```
<rule name="rpc" type="boolean" default="false" value="true"/>
```

- **formRender** - Overrides page format when a form appears on a page.

```
<rule name="formRender" type="boolean" default="false" value="true"/>
```

- **formSubmit** - Overrides page format when a form is submitted.

```
<rule name="formSubmit" type="boolean" default="false" value="true"/>
```

> **Note**
>
> The *args* value will only show what was changed by the form submission.

- **content** - Open entry for adding a special audit point.

```
<rule name="content" type="boolean" default="false" value="true"/>
```

Hint

The *use* rule (`<rule name="use" type="boolean" default="false" value="true"/>`) disables all auditing when its value is set to `false`.

Audit log message contents

Audit log messages consist of a single line and include the following fields:

1. **IP-Address**: IP address of the client provided by the web server.
2. **Mode**: Either `r` (read), `w` (write), or `x` (execute).
3. **User(id)**: Username and serial_id of the user.
4. **Page**: The page requested.
5. **Args**: Either the *rpc* command and its arguments or the fields of the form.

Audit logging to external syslog

If desired, Endpoint Analytics can also be configured to send audit log messages to a remote syslog server.

To enable audit logging to an external syslog server, do the following:

1. Run the following command:

```
# sudo vi /etc/syslog.conf to edit /etc/syslog.conf
```

2. Find the line `#*.* @log.host.address` and uncomment it by deleting the `#`.
3. Replace `log.host.address` with the IP address or FQDN of the syslog server to which audit log messages should be delivered.
4. Save the changes to `syslog.conf` and restart the syslog process by running:

```
#service rsyslog restart
```

4.3 Features and Functionality

Dashboard

Customizable widgets and at-a-glance system data visualizations

Dashboard **Endpoints**

Inspect and manage endpoint data views, profiles, and download data for offline analysis

Endpoints **Configuration**

Configure and modify Endpoint Analytics' settings

Configuration **Utilities**

Additional tools for performing administrative tasks

Utilities **Reports**

Quick access to predefined reports generated from aggregated endpoint and profile statistics

Reports

4.3.1 Endpoint Analytics UI

The Endpoint Analytics web interface offers a streamlined and intuitive platform for managing and monitoring all connected devices within a network. It is accessed by pointing any supported browser to the DNS or IP address of the appliance's management interface. The embedded web server is secured with HTTPS and supports the use of SSL certificates for verification. URLs can also be automatically redirected to HTTPS.

This section introduces the different pages and views of the web interface and provides detailed instructions for leveraging their associated functions.

4.3.1.1 Dashboard

The **Dashboard** tab/page is the web interface's landing page upon login and consists of an at-a-glance summary of the state of the entire Endpoint Analytics system.

This page allows individual users to configure their layout to display the endpoint, profile, and system data visualizations best suited to their workflows and gives them convenient access to critical statistics and data.

Clicking the **Edit** button will put the dashboard into edit mode, where the user can add, remove, and resize the following widgets to tailor the layout to their specific usage scenario:

- 24-hour Event Stats
- Connection Types
- Custom Data Names
- DHCP Client FQDNs
- DNS Zones
- Endpoint Directory
- Endpoint Stats
- Endpoints by Profile
- Endpoint Risk Levels
- MAC Vendors
- Endpoints by Risk
- RADIUS Authentication Status
- Healthcare Endpoints
- Healthcare Endpoints - Make/Model

Clicking a widget or one of its elements drills down into the endpoint or profile data displayed and brings up more detailed information. Additional details can also be viewed by mousing over widget elements.

> **Hint**
>
> Dashboard layouts and settings are saved per user and will be loaded upon login.

The Endpoint Analytics web interface also includes the following helpful features:

System status overview
The help/question mark button in the web interface's banner opens an overview of the status of the Endpoint

Analytics system, its individual software components, and any connections to Active Directory, DNS servers, or other third-party services.

Streamlined access to help and support
The **Request Support/System Status** page also offers quick access to a full range of troubleshooting options and allows the user to easily contact Plixer Technical Support or access their support portal.

4.3.1.2 Endpoints

The **Endpoints** tab/page in the web interface functions as a single pane-of-glass endpoint monitoring and administration tool that streamlines how users inspect, track, and manage endpoints on their networks. It allows the user to switch between different endpoint data views and includes options to download data for offline analysis.

Endpoint profiles

Endpoint Analytics' endpoint profiling engine actively anaylzes all discovered devices and monitors network activity to assign each endpoint a profile based on collected data. These profiles (and profile groups) are used by the web interface to provide quick access to essential endpoint data and simplify device management processes.

How profiles are assigned

The system relies on several collector modules that use various means to collect endpoint and traffic data, which are forwarded to a central server module. The endpoint profiling engine then aggregates the data for processes and uses it to assign profiles to all discovered endpoints.

Endpoint Analytics uses MAC addresses as the primary identifier for endpoints, but in certain scenarios, the IP address is the sole identifier available. In such cases, only "IP-learned" attributes can be captured for use by the endpoint profiling engine.

> **Note**
>
> When assigning profiles and monitoring the network edge for changes, Endpoint Analytics prioritizes "MAC-learned" over IP-learned attributes and will always rely on the former, when available, to make decisions and resolve conflicts.

Profiles that are assigned to similar endpoints are further grouped into factory-defined profile groups for more efficient sorting and management within the web interface.

Endpoint identity attributes

The following table lists all identity attributes used by Endpoint Analytics' endpoint profiling engine to compare against profile rules for endpoint classification:

Note

In the web interface, an endpoint's profile match score indicates the relative degree of certainty that the endpoint has been assigned the correct profile. The profile match score is also used by Endpoint Analytics to determine if and when an endpoint should be moved out of and/or into a new profile assignment.

Attribute	Description	IP-learned only?
Active Directory	Endpoint data maintained in Active Directory (domain membership, AD computer name, OS, OS version, service pack, AD domain name)	No
Custom data	User-defined attributes	No
DHCP client FQDN	Fully qualified domain name included in the DHCP request	No
DHCP client vendor	Unique vendor class identifier included in the DHCP request	No
DHCP hostname	Hostname included in the DHCP request	No
DHCP requested options	Additional options requested in the DHCP request (Option 55/81)	No
DHCP options	Full list of DHCP options supported by the client included in the DHCP request	No
DNS name	DNS name the IP address resolves to via reverse lookup	Yes
Discovery protocol	Data in the LLDP/CDP message that identifies the device to upstream neighbors	No
IP address	Full host (or subnet) address being used by the endpoint	No
MAC address/vendor	Full MAC address of the endpoint or OUI of the device manufacturer	No
RADIUS accounting data	RADIUS username of the endpoint (successful RADIUS authentication required)	No
Server banner	Contents of web/SMTP server banner returned by the endpoint to connecting clients	Yes
SNMP system description	Contents of SNMP system description collected from devices polled	No
Stack information	TCP stack parameters observed by Endpoint Analytics when the endpoint opens a TCP connection with another endpoint (TTL, window size, TCP options list)	Yes
Open TCP ports	TCP ports observed to be accepting after traffic analysis	Yes
Network traffic	Characteristics observed in communications with other hosts on a specific UDP/TCP port	Yes
Web URL	URL visited via HTTP	Yes
Web user agent	HTTP user agent string obtained through a browser	Yes
Dicom association (healthcare)	Medical imaging-specific attributes	No
Device identifier (healthcare)	Attributes linked to medical device hardware details	No
Make and model (healthcare)	Attributes linked to medical device identifier details	No

Endpoints menu

The **Endpoints** menu group of the Endpoint Analytics web interface allows the user to toggle between a wide range of sorting and viewing options in order to quickly look up profiles, profile groups, and other vital endpoint data.

Clicking on a link in any of the views will either drill down into the category or, in the case of MAC and IP addresses, open the Endpoint Summary page for that endpoint.

> **Note**
>
> In the main page of each view, groupings (profiles, profile groups, MAC vendors, etc.) that do not contain any discovered endpoints will not be displayed.

Directory

The *Directory* view lists all currently enabled profiles that have at least one endpoint, along with their profile groups and the number of endpoints that have been assigned that profile. The table also includes a **Not Profiled** category for endpoints that have been discovered but have not yet been assigned a profile.

To view the endpoints under a profile as well as additional details about them, click on the profile name on the main **Endpoints Directory** page.

By Network Device

The *By Network Device* view lists all network infrastructure device (NID) groups and the number of endpoints associated with each one. Clicking on a group name will bring up a table of all network devices in that group as well as their IP addresses.

From there, click on the IP address of an NID to view a list of all endpoints connected to the device, sorted by port number.

The *Query Now* button on this page will trigger an immediate SNMP poll and update the Endpoint Analytics database with the latest device data.

By Profile Group

The *By Profile Group* view lists all profile groups and the number of endpoints that have been assigned profiles within each group.

To view a table of all profiles and endpoints under a group, click on the profile group name.

By MAC Vendor

The *By MAC Vendor* view lists all MAC Vendor names and the number of endpoints registered with each MAC Vendor ID (OUI).

To view all endpoints with the same OUI, click on the MAC Vendor name in the list.

By Computer OS

The *By Computer OS* view lists all operating systems (OSs) currently used by discovered devices and the number of endpoints using each OS.

To view all endpoints using a specific OS, click on the OS name in the list.

By Computer Domain Names

The *By Computer Domain Name* view lists all domain names used by discovered endpoints and the number of endpoints that belong to each domain.

To view all endpoints belonging to a specific domain, click on the domain name in the list.

By Custom Data

The *By Custom Data* view lists all custom data objects that have been attached to endpoints and the number of endpoints associated with each one.

To view all endpoints with the same custom data object attached, click on the custom data string in the list.

By RADIUS Usernames

The *By RADIUS Username* view lists all RADIUS usernames used for authentication with discovered endpoints.

To view all endpoints tied to a specific RADIUS username, click on the name in the list.

Risk

The *Risk* view lists all endpoints, along with their assigned profiles and a breakdown of individual risk scores by assessment tool/service.

> **Note**
>
> A - in one of the risk columns for an endpoint indicates that no risk data is available for that source.

By VLAN

The *By VLAN* view lists all NID groups and the number of VLANs under each group. Clicking on an NID group name will bring up a table of the VLANs belonging to the group and the number of profiles associated with each one.

To view a list of profiles associated with a specific VLAN, click on the VLAN name in the list.

Network Topology

The *Network Topology* view displays a graphical representation of the network as discovered by Endpoint Analytics. The main page displays all NID groups containing devices with connected endpoints as well as an *Ungrouped* category for devices that have not been assigned to any NID groups. From there, the different elements of the visualization can be used to drill down and view the NIDs in each group and the endpoints connected to each one.

> **Hint**
>
> NIDs that have been polled recently will be displayed in green, while those that have been unreachable since they were added will be displayed in red.

IP-Only Endpoints

The *IP-Only* view lists all profiles assigned to endpoints that have not yet been mapped to their corresponding MAC addresses. The main table can be filtered by subnet group (requires the subnet groups to have been previously added).

From the main table, clicking on a profile name will display a page with all IP-only endpoints under that profile, where clicking on an individual IP address will bring up the Endpoint Summary Page.

Retired

The *Retired Endpoints* view lists all profiles assigned to endpoints that have been inactive for the configured endpoint timeout setting and flagged as retired.

> **Hint**
>
> For additional information about retired endpoints and the endpoint timeout setting, see the *data processing section* of the *Endpoint Analytics configuration guides*.

From the main table, clicking on a profile name will display all retired endpoints under that profile, along with their last known IP, profile match score, last location, and the date they were retired.

Unconnected Ports View

The *Unconnected Ports View* option displays a list of all device ports that have been reported as being down during the most recent SNMP poll sorted by the NIDs they're attached to.

Clicking on either the name or IP address of an NID will open the Edit Network Device page.

View Endpoint Events

The *View Endpoint Events* option displays a history of all events triggered by endpoints discovered by Endpoint Analytics. An event's details and management options will be accessible from this page until it is manually cleared from the system or automatically removed due to the event history setting.

To manually clear events from the system, tick the corresponding checkboxes in the first column of the table, and then click the **Delete Selected** button. Individual endpoints can also be cleared from their Endpoint Summary page.

Endpoint Summary page

The **Endpoint Summary** page contains all current and historical information about each endpoint discovered by Endpoint Analytics and can be accessed from any view or page in the web interface that contains links to an endpoint's MAC or IP address.

This page also allows the user to manually clear or delete the endpoint from the Endpoint Analytics database or add custom data objects using the buttons near the bottom of the page.

The Endpoint Summary page is divided into the following tabs:

Endpoint Summary

The main tab contains a high-level overview of all endpoint details, including:

- Profile match score for the currently assigned profile
- Risk level
- VLAN information extracted from RADIUS accounting data
- Any custom data objects associated with the endpoint

The *Show Other Profiles* link will display all other profiles that were considered by the Endpoint Profiling Engine but not used due to lower profile match scores.

Hint

If Microsoft Defender integration has been configured, the main Endpoint Summary tab will also include a link to the Microsoft Defender overview for the endpoint as well as additional buttons to scan, isolate, or unisolate the device.

Note

Endpoints connected via a Cisco hybrid wireless access point will be labeled as such under their *Current Location* details. When inspecting device ports, this will be displayed in the **Wireless Endpoint View** tab.

Risk

The **Risk** tab contains a summary of all risk information for the endpoint, with subtabs for individual risk assessment tool reports.

Profile Data

The **Profile Data** tab contains additional profile-related details for the endpoint and is further divided into seven subtabs for the following information:

- **DHCP** - DHCP lease requests and response data observed by the system
- **Active Directory** - Microsoft AD data items (only available if the system has been configured to collect data from AD servers on the network and AD information has been linked to the endpoint)
- **RADIUS** - Any RADIUS accounting information forwarded from RADIUS clients on the network (if configured)
- **Software** - Information collected if open port, user agent, web and SMTP server banner, and/or web URL data have been captured
- **Traffic** - Endpoint communications that have matched configured traffic profile rules
- **Healthcare** - Healthcare-specific device data associated with the endpoint
- **Miscellaneous** - Network stack information collected for the endpoint

Endpoint Events

The **Endpoint Events** tab lists all events triggered by the endpoint throughout its migration between profile assignments, as well as additional details for each event. For more information on events in Endpoint Analytics, see the subsection on configuring events.

MAC History

The **MAC History** tab contains all historical data tied to the MAC address of the endpoint, divided into three subtabs:

- **MAC History by Port** - Lists the network device ports the endpoint has been connected to
- **MAC History by IP** - Lists all IP addresses used by the endpoint
- **MAC History by Profile** - Lists all profiles that have been assigned to the endpoint

IP History

The **IP History** tab contains all historical data tied to the current IP address of the endpoint, divided into two subtabs:

- **IP History by MAC** - Lists all MAC addresses that have used the current IP address
- **IP History by Profile** - Lists all profiles that have been assigned to endpoints using the current IP address

> **Note**
>
> The period of time covered by the MAC and IP history data for an endpoint can be adjusted by changing the *Historical Limit* setting. For more information and instructions, see the *data processing section* of the *Endpoint Analytics configuration guides*.

Risk assessment

Endpoint Analytics evaluates endpoint risk by applying multiple assessment methods to the data collected by the system.

Endpoints are assigned an overall risk level based on the following risk assessment methods and solutions:

Risk Assessment Method	Description
Identity-Based Risk: Identity	Based on security vulnerability information associated with the endpoint's assigned profile
Identity-Based Risk: OS	Based on security vulnerability information associated with the endpoint's operating system
Duplicate MAC	Based on the detection of identical MAC addresses at multiple wired locations (expires after 24 hours) or both wired and wireless (persistent)
Tenable	Based on highest endpoint risk vulnerability discovered by a Tenable.io (if enabled)For additional information and configuration instructions, see the subsection on Tenable.io integration.
Microsoft Defender	Based on highest endpoint risk vulnerability reported by Microsoft Defender (if enabled)For additional details and configuration instructions, see the subsection on Microsoft Defender integration.

The overall risk level and individual risk scores by assessment are listed under the **Endpoints** > **Risk** view.

4.3.1.3 Configuration

The **Configuration** tab contains different submenus that allow Endpoint Analytics' various features and functions to be configured or modified. For more information on the different **Configuration** submenus, see the *Configuration Guides* section of this manual.

4.3.1.4 Utilities

The **Utilities** tab contains additional tools for searching for or displaying endpoint data and allows the user to backup the database and view system log data.

Search

The **Utilities** > **Search** submenu of the web interface comprises additional search functions that allow the user to quickly look up endpoints, profiles, and other related data.

The **Search** submenu has three different search options:

Advanced Search

The **Advanced Search** page complements the quick search tool in the web interface banner by allowing the user to perform search operations involving different comparison operators and endpoint attributes. The user is also able to build more complex database queries by using any combination of endpoint attribute filters with the logical operators AND and OR.

> **Note**
>
> Advanced search results will not include records for IP-only endpoints.

The user can also perform the following actions from the results page:

- **Refine Search** - Return to the main **Advanced Search** page to add or change search parameters
- **Edit Columns** - Show or hide data columns in the search results
- **Save** - Save the current search configuration for later use (Use the *Load a Saved Search* dropdown to select a search query to load)

Endpoint History

The **Endpoint History** option of the **Search** submenu allows the user to view the saved historical data for a MAC (by port, IP, or profile) or IP address (by MAC or profile).

In an 802.1X-enabled network, the *User History* query can be used to search for usernames that have been authenticated on the switches polled by Endpoint Analytics and view all switch port(s) through which a username has been successfully authenticated.

Data Search

The **Data Search** option can be used to search for endpoints using categories that are not covered by other search options, such as hostnames, system descriptions, and web user agents.

The *Data* column of the search results displays the data items that matched the query string, while MAC and IP addresses are direct links to Endpoint Summary pages.

Utilities menu

In addition to the Search submenu, the **Utilities** menu group contains several other data management and troubleshooting tools for Endpoint Analytics:

Profile Data

Allows the user to search for and/or view identity attributes that have been captured from discovered endpoints and drill down into the profile data to inspect the MAC or IP addresses associated with an attribute

Custom Data

Allows the user to add custom data objects to a MAC address, view (and/or edit) all custom data objects, or import custom data objects in bulk from a CSV file

A template for the batch import CSV file can be downloaded from the **Import Custom Data** page.

System Summary

Displays top-level system statistics and provides access to the following troubleshooting tools:

- **Display Server Log** - Shows the last 500 entries in the server module log file (most recent first)
- **Backup Database** - Creates a snapshot of the database, including all configuration and endpoint data, and saves the database backup file to a PC or file share as a GZIP (.gz) file
- **Cleanup Database** - Permanently deletes all web user agents, open TCP ports, and traffic data not currently being used
- **Enable/Disable Automated Database Cleanup** - Enable or disable automated database cleanups

Licenses

Lists all third-party license acknowledgements for Endpoint Analytics

Update Registered MAC Vendors

Allows the user to update the appliance's OUI table (used to resolve MAC vendors) with the latest available data published by the IEEE

If the appliance is not able to access the Internet, download the latest IEEE OUI file, extract `ieee.txt` to the workstation, and select the file using the *Update from File* option.

> **Note**
>
> A re-model is required to apply the latest changes whenever the table of registered MAC vendors is updated.

4.3.1.5 Reports

The **Reports** tab of the web interface is designed to offer quick access to a number of predefined reports, which are generated after aggregating and analyzing endpoint and profile statistics.

All reports include links that allow the user to drill down into the category and/or view the Endpoint Summary page for a MAC or IP address.

> **Hint**
>
> The **Reports** menu is an alternative means of opening the pages linked to in the web interface's dashboard widgets and can be used to access the statistics and data even when the corresponding widgets are not being used.

The following reports are available from the submenu:

- **DHCP Client FQDN Statistics**: Displays statistics for DHCP client FQDNs grouped by domain name
- **Endpoint Names**: Lists all endpoints for which at least one of the following name attributes has been discovered: DNS name, DHCP hostname/domain name/FQDN, or Active Directory DNS name
- **Endpoint Statistics**: Summarizes statistics for all discovered endpoints, split into the following tabs: Profile Name, MAC Vendor, DNS Name, OS, Domain Name, and RADIUS User Name
- **Endpoints by Connection Type**: Shows the distribution of discovered endpoints by network connection type in a pie chart
- **Endpoints by Profile - Top 10**: Shows the top ten profiles based on the number of endpoints using that assignment in a pie chart

- **Healthcare Endpoints**: Lists all healthcare-related endpoints discovered on the network, split into two tabs: Device Information and HL7 UDI (Unique Device Identifier)
- **Healthcare Imaging Endpoints**: Lists all healthcare imaging endpoints discovered on the network, along with the IP address and AE title information for each imaging device
- **Profile Statistics**: Displays a summary of profile statistics with profile groups and distribution percentages in table format
- **RADIUS Authentication**: Shows the distribution of endpoints by RADIUS authentication status in a pie chart

4.4 Advanced Services

Command Line Operations

beaconctl commands, database operations, and system maintenance functions

Command line operations **REST APIs**

Integrate with Endpoint Analytics using REST API calls

REST APIs **Integrations**

Integrate with Tenable.io, Microsoft Defender, and third-party SSO providers

Integrations **Version Upgrades**

Upgrade procedures and instructions

Version upgrades

4.4.1 Command line operations

Endpoint Analytics supports command line operations for certain appliance-level administration actions and functions, even after the system has been fully deployed and configured.

To access the command line, start a console or SSH session to the management interface (ens160) of the Endpoint Analytics appliance.

As a security measure, attempts to log in as the `root` user will be blocked by the appliance. To issue commands requiring root privileges, initiate the SSH session as the `beacon` user before elevating to root.

Hint

The password for the `beacon` appliance user account can be changed using the `passwd beacon` command.

4.4.1.1 beaconctl command set

The `beaconctl` command set is used to initiate various system-level operations from the command line. These commands primarily control the appliance software and run certain configuration scripts.

Note

All commands apart from `help` and `status` require root privileges.

The `beaconctl` script is located in `/user/beacon` on the appliance and can be used with the following options:

Option	Function
`status`	Returns the appliance software version and the current state of each system component as either *running* or *not running*
`start`	Starts all of Endpoint Analytics' software components
`stop`	Stops all of Endpoint Analytics' software components
`restart`	Stops all software components and restarts them immediately after
`config`	Re-runs the Endpoint Analytics appliance's initial configuration script
`setupnetwor`	Re-runs the script to configure Endpoint Analytics' network interface settings (ens160 IP, mask, gateway, and name server)
`setupntp`	Re-runs the script to configure Endpoint Analytics' NTP server settings
`help`	Displays help for `beaconctl` command usage

When re-running any of the configuration scripts, the user will be prompted to confirm whether to proceed with the re-configuration. At the end of the script, the system will automatically be restarted.

4.4.1.2 Additional CLI operations

In addition to the functions supported by the `beaconctl` command set, there are several other appliance-level operations that can only be performed via command line:

Clean appliance reboot or shutdown

These commands are used to gracefully shut down the Endpoint Analytics appliance (physical or VM) prior to powering it off. Performing a clean shut down or restart will ensure that the system is able to complete all running disk operations and close the database before it is powered down.

To completely shut down or power off the appliance, issue the following command with root privileges:

```
shutdown -p now
```

To reboot/restart the appliance, issue the following command with root privileges:

```
shutdown -r now
```

Database restoration

The Endpoint Analytics database is automatically backed up on a daily basis and can also be backed up manually from the *System Summary page* of the Endpoint Analytics web interface.

To restore the database from a backup, follow these steps:

1. Copy the database backup file to `/backup` on the appliance (if not already present there) using secure copy protocol (SCP)

> **Hint**
>
> To perform a system restore from the most recent database backup, use the symbolic link `dailyDB-latest.gz` in the `/backup` directory.

2. Open an SSH session to the appliance, change directory to `usr/beacon/scripts/maint` and run the following script:

```
./restoreDB.pl /backup/<backup_filename>
```

3. After running the script, navigate to **Configuration > Data Processing** in the web interface, and then click the **Re-model** button to refresh the system using the restored database.

By default, the script will automatically restart all system modules before it finishes running. To disable this, add the `-nostart` switch to the command line.

Database autotuning

The Endpoint Analytics database is automatically tuned to suit available system resources during the initial installation process.

The autotuning script can also be run manually when and as needed via CLI.

To run the script, open an SSH session to the appliance and change directory to `/usr/beacon/scripts/maint`.

From there, run the following script:

```
./db_config_manager
```

The database autotuning script has the following settings that can be changed:

Setting	Description	Flag
Auto	Adjusts postgresql.conf automatically based on hardware	-a
Reset	Resets postgresql.conf to factory default	-r
Size	Deploys preconfigured postgresql.conf based on standard database sizing	-s (S|M|L)
Help	Displays command help	-h

4.4.2 REST APIs

Endpoint Analytics supports REST API calls to search its database for endpoint, user account, device, and profile data.

4.4.2.1 API documentation

The API documentation can be generated by running a script on the appliance and viewing the pages in a standard browser.

To generate the API documentation, follow these steps:

1. Open an SSH session to the appliance as the `beacon` user and elevate to root.
2. Change directory to `/usr/beacon/www`.
3. Run the following command:

```
# php artisan scribe:generate
```

Once the script has finished running, open the URL `https://<appliance_ip>/docs` in any browser to view the API documentation pages.

4.4.2.2 API debugging

To enable API debugging, run the following command:

```
# sed -i -e "s/'debug' => \!\$inUsr,/'debug' => \$inUsr,/g" /usr/beacon/www/config/app.php
```

To disable API debugging, run the following command:

```
# sed -i -e "s/'debug' => \$inUsr,/'debug' => \!\$inUsr,/g" /usr/beacon/www/config/app.php
```

4.4.3 Integrations

Endpoint Analytics supports multiple third-party integrations that further enhance the system's capabilities.

4.4.3.1 Tenable.io

When enabled, Tenable.io integration allows Endpoint Analytics to pull vulnerability data from the scanning service and use it to assign a risk level to endpoints discovered on the local network.

After configuring the integration, Tenable.io risk metadata will be taken into account when assigning an overall risk level to an endpoint. A **Tenable.io** subtab containing the following will also become available under the **Risk** tab of **Endpoint Summary** pages:

- Risk level badge based on the highest risk vulnerability discovered by the service
- Hyperlink to Tenable.io asset activity page for the endpoint
- Hyperlink to Tenable.io asset vulnerability page for the endpoint

In addition, all assets that are known to both Endpoint Analytics and Tenable.io will be listed under the **Endpoints by Risk** view, including those with no risk/vulnerabilities reported by Tenable.io.

To configure Tenable.io integration, follow these steps:

View instructions

1. Navigate to **Configuration** > **Integrations**, and then select **Tenable.io** to open the configuration page.
2. Fill in the fields with the Tenable.io access key and secret key.
3. Tick the **Enabled** checkbox, and then click **Test Connection** to verify the credentials entered.
4. When done, click the **Save** button to save the configuration.

4.4.3.2 Microsoft Defender

When enabled, Microsoft Defender integration enables the following functions in Endpoint Analytics:

- Pull external OS risk data from the risk analysis platform and use it to assign a *risk level* to endpoints discovered on the local network
- Import MS Defender machine inventory as endpoints
- Automatically create and assign dynamic profiles (named `OS` or `OS_VERSION`) to imported endpoints whose OS details are provided by MS Defender

After enabling the integration, MS Defender vulnerabilities will be factored into an endpoint's overall risk level. Endpoints with risk factors reported by MS Defender will include a hyperlink to the MS Defender overview page in their *Endpoint Summary*. MS Defender actions (*Run Scan*, *Isolate Machine*, and *Unisolate Machine*) will also be available for supported devices that have been onboarded in MS Defender.

Additionally, a *Microsoft Defender* subtab containing the following information will be added under the **Risk** tab of **Endpoint Summary** pages:

- Description of the most severe vulnerability found via Microsoft Defender Exposure assessment and a corresponding Exposure Risk Level badge
- Number of vulnerabilities, which also links directly to the endpoint's Microsoft Defender vulnerabilities page
- Risk Level badge based on the most severe alert found via Microsoft Defender Risk assessment
- Hyperlink to Microsoft Defender risk alerts page for the endpoint
- Hyperlink to Microsoft Defender overview page for the endpoint

Note

- Machine inventory information is collected hourly, starting from when MS Defender integration is enabled.
- Imported endpoints will always have a *Very High* profile match score against the automatically created OS-based profiles. Imported endpoints for which MS Defender does not provide OS details will be *assigned profiles as normal*.
- If MS Defender integration is disabled, all associated profiles are deleted. Imported endpoints are retained and will be assigned standard profiles instead (requires a *full re-model*).

Configuring MS Defender integration

Follow the process outlined below to set up and enable MS Defender integration in Endpoint Analytics.

Creating an application

To set up an application to allow Endpoint Analytics to access MS Defender, follow these steps:

1. Log in to the Azure portal with a user that has the *Global Administrator* role.
2. From the Azure Active Directory page, navigate to **App registrations > New registration**.
3. Enter a name for the application, and then click **Register**.
4. Note the application (client) ID and directory (tenant) ID.
5. Under **Certificates and Secrets**, select *New Client Secret*.
6. Enter a description and expiration date, and then click **Add**.
7. Note the client secret generated (cannot be retrieved later).

API permissions

Once added, the application will need to be granted the necessary API permissions (see below) to allow Endpoint Analytics to access the APIs.

Note

Every time a permission is added, go to the **API Permissions** page for the application and grant it admin consent (requires *Global Administrator* role) for the organization.

Following are the permissions required for the APIs used by Endpoint Analytics:

Get MachineAction

Retrieves a single machine action entity

Permission	Description
Machine.Read.All	Read all machine profiles
Machine.ReadWrite.All	Read and write all machine information

List MachineActions

Retrieves a list of machine actions

Permission	Description
Machine.Read.All	Read all machine profiles
Machine.ReadWrite.All	Read and write all machine information

List alerts

Retrieves a collection of alerts

Permission	Description
Alert.Read.All	Read all alerts
Alert.ReadWrite.All	Read and write all alerts

Isolate machine

Isolates a compromised machine from accessing external networks

Important

When isolating a machine, it will lose all network connectivity until it is released from isolation.

Permission	Description
Machine.Isolate	Isolate machine

Release machine from isolation

Undo isolation of a machine to re-enable network connectivity

Permission	Description
Machine.Isolate	Isolate machine

Run antivirus scan

Initiate a Microsoft Defender Antivirus scan on the device

Permission	Description
Machine.Scan	Scan machine

List vulnerabilities

Retrieves a list of all the vulnerabilities affecting the organization

Permission	Description
Vulnerability.Read.All	Read Threat and Vulnerability Management vulnerability information

Advanced hunting

Run queries from API to locate threat indicators and entities

Permission	Description
AdvancedQuery.Read.All	Run advanced queries

Get software by ID

Retrieves a specific software by its software ID

Permission	Description
Software.Read.All	Read Threat and Vulnerability Management Software information

List devices by software

Retrieves a list of devices that are associated with the software ID

Permission	Description
Software.Read.All	Read Threat and Vulnerability Management Software information

Enabling MS Defender integration in Endpoint Analytics

To configure and enable MS Defender integration, follow these steps:

1. In the Endpoint Analytics web interface, navigate to **Configuration** > **Integrations**, and then select *Microsoft Defender* to open the configuration page.
2. Fill in the provided fields with the MS Defender tenant ID, client ID, and client secret key.
3. Tick the *Enabled* checkbox, and then click **Test Connection** to verify the credentials entered.
4. Click **Save**.

Once the information has been saved, Endpoint Analytics will attempt to collect the necessary information from MS Defender, and all additional functions (see above) will be enabled.

Important

Azure SSO authentication within the web interface is not required to view external MS Defender pages for endpoints discovered by Endpoint Analytics. However, the user must have Azure AD Security Reader role permissions (minimum) as described here.

4.4.3.3 Third-party SSO

SSO authentication for the Endpoint Analytics web interface has been tested with the following third-party identity providers:

- Microsoft Azure Active Directory
- Google
- Okta

Important

Before configuring SSO in the web interface, the identity provider must be set to accept authentication requests from Endpoint Analytics.

To configure the Endpoint Analytics web interface to route authentication through a third-party identity provider, follow these steps:

1. Navigate to **Configuration > Identity Providers**, and then select **Add Identity Provider**.
2. On the **Add Identity Provider** page, enter the following details:
    - **Name**: Unique, internal name for the provider/service
    - **Client ID**: ID assigned to the app registration in the identity provider console (also called the application ID)
    - **Discovery Document Endpoint**: OpenID Connect metadata document URL (should end in /.well-known/openid-configuration)
    - (Optional) **Authorized Groups**: Comma-separated list of users with SSO access (no authorization restrictions if left blank)
3. Tick the radio button to select the default access level to assign when users log in for the first time (will not affect existing users).
4. Tick the **Verify Token Signature** checkbox to require verification of the integrity of tokens used during SSO (not supported by all identity providers).
5. Tick the **Enable** checkbox to activate SSO via the identity provider, and then click **Save**.

After SSO has been configured and enabled, attempts to log in via `https://<appliance_ip>` will be redirected to the identity provider currently enabled.

Managing identity providers

Selecting **List Identity Providers** from the **Identity Providers** configuration submenu will open a summary page listing all identity providers currently configured within the system.

From this page, the following actions can be performed:

- Adding a new identity provider
- Editing the settings of a configured identity provider
- Enabling/disabling identity providers
- Deleting identity provider configurations
- Exporting identity provider data in CSV format

Hint

To revert to local user authentication for the web interface, either delete or disable all identity providers. **This will delete all accounts created through SSO authentication, and only locally created accounts (and the administrator account) retain access to the web interface**.

4.4.4 Version upgrades

Updates to Endpoint Analytics may add new features, enhance existing functionality, and/or apply security patches to address emerging threats.

This section covers the installation process for update packages as well as additional recommendations for pre-upgrade preparations.

Note

All update packages are extensively tested by the Plixer team before they are made available. For assistance with the update process and other concerns, contact *Plixer Technical Support*.

4.4.4.1 Update preparations

Before attempting to install any type of update package, the following procedures should be observed:

1. Verify that the version currently installed can be upgraded to the target version.
2. Confirm that a recent *backup* has been saved or manually back up the database from the *System Summary page*. The backup file should also be copied to an external location.
3. Verify that the current license key(s) will remain valid after the upgrade.
4. Delete any older update files/packages from the home directory for the `beacon` user.

4.4.4.2 Update installation

Follow the steps below to update the current Endpoint Analytics instance to the latest version:

1. Ensure that a backup of the current install has been saved to an external location, as part of the *recommended preparatory procedures*.
2. SSH to the Endpoint Analytics instance as the `beacon` user and start a new tmux session:

```
tmux new -s upgrade
```

3. Download the update package for the latest version (will be saved in the format `pea_7.1.5_upgrade.tar.gz`):

```
curl -o pea_7.1.5_upgrade.tar.gz -L https://files.plixer.com/
↪PlixerEndpointAnalyticsUpgrade.tar.gz
```

4. Extract the contents of the downloaded file to the same (home) directory:

```
sudo tar -xvzf pea_7.1.5_upgrade.tar.gz
```

5. Navigate to the extracted directory, and then set the correct permissions for the update script:

```
cd pea_7.1.5_upgrade/
sudo chmod 755 upgrade.sh
```

6. Run the update script, and then type `yes` when prompted:

```
sudo ./upgrade.sh
```

Once the script completes running and the system reboots, the instance will be running the latest version of Endpoint Analytics.

Offline updates

To update an Endpoint Analytics instance that cannot access the Internet, follow these steps:

1. Download the update package from a system with access to the Internet.
2. Copy the package to the home directory of the `beacon` user.
3. Follow the online update procedure above starting from step 4.

Once the script completes running and the system reboots, the instance will be running the latest version of Endpoint Analytics.

4.5 Additional Resources

FAQs

Answers to frequently asked questions

FAQ **Changelog**

Endpoint Analytics updates and version history

Endpoint Analytics changelogs **Glossary**

Glossary of terms used in Endpoint Analytics

Glossary **Attributions**

Open source and third-party licenses

Third-party attributions **Plixer technical support**

Plixer Technical Support is available with an active maintenance contract. Contact our support team at:

- **Phone:** +1 (207) 324-8805 ext 4
- **Website:** https://www.plixer.com/support/

4.5.1 FAQ

Note

For additional questions or concerns, contact *Plixer Technical Support*.

If the left LED stays off, verify that you are using a working cable of the correct type and check if the switch port has been correctly configured.

These additional monitoring ports can be used to passively collect network packets. Depending on the appliance model, there may be up to four extra monitoring ports available.

Open a console or SSH session to the appliance as the `beacon` user, then enter the following command: `$ passwd beacon`

Endpoint Analytics license keys can only be obtained by contacting Plixer Support and providing your appliance's unique machine ID. License key files obtained through any other channels will not be accepted, and attempting to edit an existing license key file will likewise render it unusable.

The EULA is stored on the appliance and can be viewed at any time by opening the file `/usr/beacon/GBS-EULA.txt`

Endpoint Analytics requires only one subnet group to be defined to start collecting data. In larger deployments, however, it may be more practical to create multiple subnet groups to segment the address space into geographical, departmental, or other logical groups.

Administrator accounts have full access to all web interface features and functions, but it is highly recommended to rely on Operator and Analyst accounts for day-to-day operations.

To change or reset the password for a web interface user, use the **Edit Account** page. Users can also change their own passwords by opening the user menu and selecting *My Settings*.

All local web user accounts will remain active even after SSO has been configured and enabled. However, SSO will become the primary authentication method for all users apart from the administrator account going forward.

Once a network device has been added, its IP address can no longer be edited, and the same is true for device groups and their names. To change those details, the network device or device group must be deleted and re-added with the new or corrected information.

In the case of certain network devices (e.g., unmanaged switches, IP phones, and wireless access points), it's possible to have multiple endpoints connected to the same port, even if it isn't labeled as a trunk port.

Support for wireless LAN controllers (WLCs) and access points is currently limited to Cisco and Aruba wireless devices. When a WLC is configured as a network device, there will be three tabs when viewing device ports: **Wired View**, **Wireless Endpoint View**, and **Wireless SSID View**.

Since multiple NIDs can share the same VLAN while belonging to different NID groups, the combined total of VLANs across all NID groups will often be greater than the actual number of detected VLANs.

Endpoint Analytics supports event delivery to internal and external *syslog* servers. For additional information, see the section on *syslog event delivery*.

An endpoint whose MAC address has not yet been mapped to an IP address when the Endpoint Summary page is opened will have its IP History tab disabled.

Alarm Profile and/or Profile Consistency Events will be triggered every time an endpoint MAC is remodeled for as long as its state or behavior continues to satisfy the conditions of the event(s). Endpoints that trigger such events should be monitored closely to avoid repeated event delivery.

Endpoint Analytics only accepts custom data CSV files that are correctly formatted. If you are having issues, we recommend using the template that can be downloaded from the **Import Custom Data** page.

Endpoint Analytics uses a PostgreSQL (single) database to store all system configuration and endpoint data. The system performs an automatic backup of the database every day, at approximately 0300 system time, but manual backups can also be initiated from the System Summary page of the Endpoint Analytics web interface.

Tick the **Anonymized** checkbox in the **Backup Database** dialogue to create the backup without customer-specific identifiers.

Database backups are maintained in the `/backup` directory of the appliance with a 30-day cleanup rotation. To determine the dates when the current backup files were created, perform `ls -la` on the directory.

In case it becomes necessary to perform a full system recovery, the appliance's software image must be reinstalled before re-running the scripts to set up the basic system configuration and licensing. From there,

restoring the database will return the system to its exact state during the backup. For assistance with this process, contact Plixer support.

4.5.2 Endpoint Analytics changelogs

Changelog entries are displayed in the format **DESCRIPTION (Ticket Number)**.

> **Note**
>
> - For additional details on any of the new features below, refer to the Endpoint Analytics documentation on the Plixer website.
> - Please refer to our End of Life Policy for EOL schedule details.

4.5.2.1 Version 7.1.0 - (05/05/2023)

Changelog

New Features

- Improved framework for updates and upgrades
- Added support for Risk Score integration in Scrutinizer
- Added support for Cisco "hybrid" wireless access point endpoint locations
- Added labels to endpoints or access points using Cisco hybrid mode to their respective summary views
- Endpoints by Risk widget added to available Dashboard widgets
- Endpoints by Risk view can now be filtered by risk assessment source
- Profile Identity Scores have been replaced by Profile Match levels to better reflect what they indicate
- MAC-to-IP binding source will now be displayed under *IP Source* on the Endpoint Report page
- Custom Data can now be automatically deleted when the associated endpoint is removed
- The Utilities > Custom Data > List Custom Data view will now also display the contents of the *Description* field and include it when exporting to CSV or XML
- Tenable.io: Added support for Tenable.io asset inventory matching
- MS Defender: Device alert metadata will now be used to support an endpoint's Risk Score
- MS Defender: Additional risk details (description, number of vulnerabilities) will now be displayed in the MS Defender subtab of an endpoint's Risk tab
- License keys now only need to be pasted into a provided field instead of being uploaded as a file

4.5.2.2 Version 7.0.0 - (07/15/2022)

Changelog

New Features

- MS Defender integration
- Tenable integration
- Single Sign On
- Enhanced risk assessment

Fixes

- License information and license paths for Endpoint Analytics on Linux now show correctly (235)
- Clear endpoint function is now works correctly (280)
- Radius Authentication Report now shows the correct statuses in the pie chart (243)
- IP address hyperlinking now works correctly (282)
- Local time zone should now be displayed instead of UTC (328)

4.5.2.3 Version 6.3.0 - (09/15/2020)

Changelog

New Features

- VLAN Support
- Unassigned Custom Data

Enhancements

- Profiling Enhancements
- Network Device Management Enhancements
- API expansion
- JSON-RPC API
- REST API

4.5.3 Glossary

This glossary is meant to serve as a reference for terms and concepts used in the Endpoint Analytics system software or this product manual.

4.5.3.1 Endpoint Analytics

View content

Endpoint profiles
: General classifications assigned to endpoints by Endpoint Analytics based on identity attributes observed by the system

Endpoint profiling engine
: Software component of Endpoint Analytics that is responsible for analyzing endpoint identity attributes and assigning/reassigning profiles

Endpoint profiling and identity monitoring
: Endpoint Analytics' core functionality, where the system continuously captures identity attributes from connected endpoints to maintain an up-to-date database and alert users to irregularities in device state or behavior

Events
: Changes in an endpoint's state or behavior that may result in profile reassignment and can be used to draw attention to endpoints of interest

NetWatch
: A network monitoring tool or feature that captures and analyzes traffic directly from endpoints

Profile groups
: Logical groupings of profiles used for more efficient endpoint sorting and management in the web interface

4.5.3.2 General networking

View content

2LD (Second-level Domain)
Part of the naming convention for domain names. For example, in example.com, *example* is the second-level domain of the .com TLD (Top level domain)

3LD (Third-level Domain)
For example, in www.mydomain.com, *www* is the third-level domain

ACK (Acknowledgment Code)
A unique signal sent by a computer to show that it has successfully transmitted data

ACL (Access Control List)
A set of rules governing access to a particular object or system resource

Active Directory / AD
Proprietary directory service offered by Microsoft, which allows for centralized management of users, devices, and other IT assets

API (Application Programming Interface)
A software component that allows applications to share data and functionality

ARP (Address Resolution Protocol)
Protocol that maps a dynamic IP address to a physical machine's permanent MAC address in a local area network (LAN)

CA (Certification Authority)
A trusted entity that issues, signs, and stores digital certificates

CDP (Cisco Discovery Protocol)
Protocol used by Cisco devices to allow neighboring networking devices to learn about each other

CIDR (Classless Inter-Domain Routing)
An IP addressing method that improves the efficiency of allocating IP addresses

CLI (Command-line Interface)
A text-based interface for applications and operating systems that allows a user to enter commands

Collector
SIEMs, Flow Collectors, SNMPTrap Receivers, or other network management systems that analyze data forwarded from networked devices

DHCP (Dynamic Host Configuration Protocol)
Network management protocol used to automatically assign IP addresses and other communication parameters to devices on an Internet protocol network

DNS (Domain Name System)
A system by which computers and other devices on the Internet or Internet protocol networks are uniquely identified using names matched to their IP addresses

Egress
Traffic that exits a device or network

Endpoint
An entity (device, service, node, etc.) at the end of a network communication channel

Encapsulated Remote SPAN (ERSPAN)
Encapsulates mirrored traffic in GRE (Generic Routing Encapsulation) and sends it over Layer 3 networks

ESX (Elastic Sky X)
A pre-configured, ready-to-deploy virtual machine (VM) designed to run on VMware ESX or ESXi

Exporter
A networked device such as a router, switch, or server that generates data and sends it to the flow collector device

Fault tolerance
A system's ability to continue operating without interruptions in the event of hardware or software failure

FQDN (Fully Qualified Domain Name)
The complete address of a computer, host, or any other entity on the Internet

GRE (Generic Routing Encapsulation)
A tunneling protocol developed by Cisco Systems

Hyper-V
A pre-configured, ready-to-deploy virtual machine designed to run on Microsoft Hyper-V, typically packaged in VHD/VHDX format

ICMP (Internet Control Message Protocol)
A protocol used for devices within the network to determine possible network issues

Identity Provider (IdP)
A third-party entity and/or service that stores and manages identities and credentials for use by other websites, applications, or other digital resources

IP address
A unique numerical label assigned to a networked device

IPFIX (Internet Protocol Flow Information Export)
A protocol intended to collect and analyze the flow data from supported network devices

KVM (Kernel-based Virtual Machine)
A pre-configured virtual machine designed to run on KVM hypervisors, packaged in formats like QCOW2 or OVA for easy deployment in Linux-based virtualization environments

Latency
The latency of a network is the time it takes for a data packet to be transferred from its source to the destination

LDAP (Lightweight Directory Access Protocol)
An open, cross-platform protocol used to access and maintain directory services for assets in an Internet protocol network

LLDP (Link Layer Discovery Protocol)
A vendor-neutral protocol used by devices on IEEE 802 networks to advertise their identity, capabilities, and other information

MAC (Media Access Control) address
A unique hardware identifier typically assigned by manufacturers to network adapters and devices

MIB (Management Information Base)
A database that stores information used for managing a network

MTTR (Mean Time to Resolution)
The the average amount of time between the detection and remediation of a security threat or incident

NDR (Network Detection and Response)
A cybersecurity solution that use machine learning to detect cyber threats and aid remediation

Network interface
A (physical or software-based) point of connection between a network entity and the rest of the network

NIC (Network Interface Card)
Adapter that provides devices network connections, either wired or wireless

NID (Network Infrastructure Device)
Any device, such as an access point, router, or switch, that provide the means for entities to communicate with each other over a network

NTP (Network Time Protocol)
A networking protocol used to synchronize device clocks over the Internet

NXDOMAIN (No Existing Domain)
An error message that means that a domain mentioned in the Domain Name System (DNS) query does not exist

Open port
A TCP or UDP port that has been configured to accept packets

OUI (Organizationally Unique Identifier)
A unique 24-bit number in a MAC address that identifies the vendor or the manufacturer of the device

OVF (Open Virtualization Format)
An open source standard for packaging and distributing virtual machines and software applications

Packet
A block of data transmitted across a network

PDU (Protocol Data Unit)
An individual unit of information exchanged by entities on a network using the same protocol

PostgreSQL
An open-source relational database management system (RDBMS) that supports both SQL and JSON querying

PXE (Preboot Execution Environment)
A network booting protocol that allows computers to boot from a network rather than a local storage device like a hard drive or USB

RADIUS (Remote Authentication Dial-In User Service)
A client-server AAA (authentication, authorization, accounting) protocol used to manage remote user access to a network

Redundancy
The state of having duplicate or alternative services as backups to allow for continuous availability

REST API (Representational State Transfer Application Programming Interface)
A set of rules that allows systems to communicate over the web using standard HTTP methods

Router
A device that forwards or routes data packets to devices on a network

Server
A system or device that provides resources, data, services, or applications to other devices over a network

Single Sign-On (SSO)
A technology that enables users to access multiple applications with a single set of credentials through third-party authentication services

SIP/RTP (Session Initiation Protocol/Real Time Protocol)
SIP is the control protocol, and RTP is the payload protocol used to send and receive Voice over IP (VoIP)

SNMP (Simple Network Management Protocol)
An IP network protocol used to collect data related to state and/or behavior from devices on a network

SNMP trap
An alert message that is initiated by an SNMP-enabled device to notify the management system of significant events or changes in status

Software agent
A persistent piece of software that performs certain actions and/or interacts with its environment on behalf of a user or another program

SPAN (Switched Port Analyzer)
A dedicated port on a switch that takes a mirrored copy of network traffic from within the switch to be sent to a destination

SSDP (Simple Service Discovery Protocol)
A network protocol used for advertising and discovering network services

SSH (Secure Shell Protocol)
A network communication protocol that allows network services to be used securely over an unsecured network

SSL (Secure Sockets Layer)
A protocol for establishing secure connections between networked devices

STIX (Structured Threat Information eXchange)
An industry-standard file format for the exchange of threat information between organizations and platforms

Suricata
A network threat detection engine used to analyze network traffic and identify potential security threats

Switch
A device that connects devices in a network and allows them to communicate with each other

SYN scan
A port scanning technique that allows for the discovery of the status of a communications port without establishing a full connection

Syslog
A cross-platform network logging protocol used to send and/or receive alerts between different devices on a network

TAXII (Trusted Automated eXchange of Indicator Information)
A protocol that allows the transmission of threat information, primarily in STIX format, between systems and organizations

TACACS+ (Terminal Access Controller Access-Control System)
A protocol where the remote access server and the authentication server provide validation for users attempting to access the network

TCP (Transmission Control Protocol)
A connection-oriented protocol that enables the bidirectional exchange of messages between devices on the same network

TLS handshake
The process that starts secure communication between a client and a server

TSIG (Transaction Signature)
A protocol that secures DNS packets and allows a Domain Name System to authenticate updates to the DNS database

TTL (Time To Live)
A field in the IP packet header that specifies the maximum number of hops (or router passes) a packet can take before being discarded

UDP (User Datagram Protocol)
A communication protocol for transmitting messages between applications and programs in a network

Virtual appliance
A pre-configured virtual machine image with pre-installed software that is meant to serve a specific function

VoIP (Voice over Internet Protocol)
A technology that allows voice calls using an internet connection

VPC (Virtual Private Cloud)
A secure and private cloud hosted in a public cloud

VRF (Virtual Routing and Forwarding)
A technology that separates routing tables to isolate management traffic to the management interface

Web server banner
A text-based greeting message, which includes information like open ports, services, and version numbers, returned by a web host

4.5.4 Third-party attributions

Endpoint Analytics is redistributed with a number of open-source and/or third-party software components. In accordance with their licensing terms, the licenses can be viewed by navigating to the following files or locations on the Endpoint Analytics appliance:

- Ubuntu packages: `/usr/share/doc/*/copyright`
- Javascript dependencies: `/usr/beacon/thirdparty/javascript-licenses.txt`
- PHP dependencies: `/usr/beacon/thirdparty/php-licenses.txt`

The terms outlined therein only apply to the libraries themselves and not the Endpoint Analytics software.