Logging features of key-value pair properties

Several key-value pair properties are placed in the structured data element of a syslog entry. These properties can also be logged in the header or message elements but are difficult to parse or extract.

> Log data is set to show based on the SecureAuth Threat Service subscription level, so you might not see all of these properties in the logs.

Threat descriptions

Threats defined

Key Name	Description	Notes
AE.IP.threatType	Threat Type identifies the classification of the attack.	See Threat Types below for more information.
AE.IP.threatCategory	Threat Category identifies the attacker method.	See Threat Categories below for more information.
AE.IP.geoContinent	Continent identifies the location of the IP address: Africa, Antarctica, Asia, Australia, Europe, North America, Oceania (Melanesia, Micronesia, Polynesia), South America.	
AE.IP.geoCountry	Full country name is used within the ISO-3166Alpha-2 code system.	
AE.IP.geoCountryCode	International Standard Organization's 2-letter code corresponds to the name of the country, as defined in ISO-3166.	
AE.IP.geoCountryCF	Country Confidence Factor – from 0 (null) to 99 – reflects a relative measure of certainty the user is in the location identified in the country field. The higher the value, the greater the likelihood that the user is in the assigned country.	
AE.IP.geoRegion	Directional Region information (e.g. 'northwest') for some countries, or specific regional information (e.g. 'northern_ireland') for a few other countries. Region information is currently available for the U.S., U.K., Brazil, Denmark, France, Philippines, Belgium, Burkina Faso, Equatorial Guinea, Greece, Guinea, Indonesia, Ireland, Italy, Malawi, Marshall Islands, New Zealand, Slovenia, Spain, Sri Lanka, and Uganda.	
AE.IP.geoState	IP Intelligence provides information for states and provinces (i.e. first-level administrative division) in all countries where they exist. NOTE: IP Intelligence uses the localized spelling for state values. For example, the state of Tuscany in Italy is identified as ‘toscana’ in GeoPoint data. This approach ensures the highest degree of system compatibility, as well as the ability to use localized state names for customer applications serving those countries.	
AE.IP.geoStateCode	State Code is the abbreviated code that identifies a state or province.	
AE.IP.geoStateCF	IP Intelligence provides a State Confidence Factor that reflects a relative measure of certainty that the user is in the location identified in the state field. Values range from 0 (null) to 99. The higher the value, the greater the likelihood that the user is in the assigned state.	
AE.IP.geoCity	IP Intelligence locates users in respective cites and recognizes more than 150,000 distinct international locations. NOTE: IP Intelligence uses the localized spelling for city values. For example, the city of Rome in Italy is identified as ‘roma’ in GeoPoint data. This approach ensures the highest degree of system compatibility, as well as the ability to use localized state names for customer applications serving those countries.	
AE.IP.geoCityCF	IP Intelligence provides a City Confidence Factor that reflects a relative measure of certainty that the user is in the location identified in the city field. Values range from 0 (null) to 99. The higher the value, the greater the likelihood that the user is in the assigned city.	

AE.IP.geoPostalCode	Postal Code is assigned to a corresponding city. Most of GeoPoint's postal code assignments are derived from the city field. Where there is sufficient evidence, the postal code is explicit. IP Intelligence provides postal codes for most countries.	
AE.IP.geoAreaCode	Area Code is the phone number prefix assigned to its corresponding city. Prefixes are available in the U.S., Canada, and selectively in other countries. NOTE: 'area_code' does not include the telephone country code.	
AE.IP.geoTimeZone	Time Zone is provided as a +/- offset of Greenwich Mean Time (GMT) and is represented as a floating point number so that calculations can be made for a specific time in a designated location. Values can be between -11 and 13. The time zone is derived from the city field, if known, or from the country field if the city is unknown. If city is unassigned and the country spans multiple time zones, a value of '999' is returned.	
AE.IP.geoLatitude	Latitude of the identified GeoPoint location is expressed as a floating point number with range of -90 to 90. Positive numbers represent North and negative numbers represent South. Latitude and longitude are derived from the city or postal code.	
AE.IP.geoLongitude	Longitude of the identified GeoPoint location is expressed as a floating point number with range of -180 to 180. Positive numbers represent East and negative numbers represent West. Latitude and longitude are derived from the city or postal code.	
AE.IP.dma	Defined Market Area (DMA) codes are assigned to geographical regions in the U.S. where the population typically receives similar media: e.g. radio, television, newspapers, and the Internet. The code, which is based on Nielsen's market codes but has parity with Google's metropolitan area codes, defines geographical areas that may coincide and overlap with one or more metropolitan regions. For example, San Francisco, San Jose, and Oakland all fall into the same DMA.	
AE.IP.msa	Metropolitan Statistical Area (MSA) codes represent geographical boundaries of U.S. counties or towns that use Core-Based Statistical Areas (CBSAs) defined by the U.S. Office of Management and Budget (OMB) from data gathered by the U.S. Census Bureau.	
AE.IP.connectionType	Connection Type pertains to ways in which users can connect to the Internet: fiber optic connections, leased line, high-speed or broadband, frame relay circuits, DSL, cable modem broadband circuits, Integrated Services Digital Network, dial-up modem, fixed wireless connections, cellular network providers, and unknown means.	
AE.IP.lineSpeed	Connection speed to the Internet is divided into categories of high, medium, or low, as determined by the Connection Type.	
AE.IP.ipRoutingType	IP Routing Type (IPRT) specifies how the connection is routed through the Internet and can be used to determine how close the user is to the public IP address. For example, a user connecting through a fixed connection is likely very close to the connection. A user connecting through a regional proxy is probably in the same country as the connection, whereas a user connecting through a satellite connection could be anywhere.	
AE.IP.geoAsn	Autonomous System Number (ASN) is a globally unique number assigned to a group of networks administered by a single entity such as a Network Service Provider (NSP) or a very large organization. ASNs manage data routing via the Border Gateway Protocol (BGP). IP Intelligence provides ASN information in 32-bit integer format.	
AE.IP.sld	Second-Level Domain (SLD) is the part of the domain name that precedes the top-level domain. E.g. in www.companyname.com, "companyname" is the second-level domain.	
AE.IP.tld	Top-Level Domain (TLD) identifies the most general part of the domain name in a Web address. Common top-level domains include com, net, edu (educational), mil (military), as well as country codes like jp (Japan) and fr (France).	
AE.IP.organization	The Registering Organization is the entity responsible for the actions and content associated with a given block of IP addresses. This function is in contrast to that of the carrier, which is responsible for routing traffic for network blocks. Registering Organizations include many types of entities, including corporate, government, or educational entities, and ISPs managing the allocation and use of network blocks.	
AE.IP.carrier	Carrier provides the name of the organization that owns the ASN and is responsible for traffic flowing on the network or set of networks designated as an Autonomous System (AS) and identified by the ASN. While there are more than 27,000 active ASNs, there are fewer carriers, because a single carrier often manages several ASNs.	
AE.IP.anonymizer_status	A status is assigned to an IP address detected as a proxy and indicates the IP address may be associated with an anonymizing proxy. The status is a relative indicator of how recent the proxy was found to be active and the proxy's category.	
AE.IP.proxyLevel	Proxy Level describes the degree of concealment for the end user via use of the proxy: e.g. obfuscation of the user's originating IP address. Levels of obfuscation include: transparent, anonymous, distorting and elite.	
AE.IP.proxyType	Proxy Type describes the network or protocol used by the server to proxy the user connection. Classifications include the use of HTTP, Tor, Web and SOCKS.	

AE.IP.proxyLastDetected	Proxy Last Detected provides the most recent date on which IP Intelligence proxy detection technology confirmed the proxy was active or served as a private proxy. This information supplies more granular proof that an IP address may be associated with an anonymizing proxy.	
AE.IP.hostingFacility	Hosting Facility identifies whether the connection originated at a facility that provides storage, computing or telecommunication services. The designation of a 'hosting_facility' includes the following type of service providers: colocation, cloud computing, dedicated hosting, virtual private servers and Web hosting.	
AE.IP.RiskScore	Risk Score is based on IP Address evaluation and threat intelligence data.	Applicable only to IP reputation log entries. Also logged in the message element.

Example of threat description log entry

```
AE.IP.threatType="100"
AE.IP.threatCategory="0"
AE.IP.geoContinentDescription="asia"
AE.IP.geoCountryDescription="thailand"
AE.IP.geoCountryCodeDescription="th"
AE.IP.geoCountryCFDescription="99"
AE.IP.geoRegionDescription=""
AE.IP.geoStateDescription="krung thep"
AE.IP.geoStateCodeDescription=""
AE.IP.geoStateCFDescription="85"
AE.IP.geoCityDescription="bangkok"
AE.IP.geoCityCFDescription="72"
AE.IP.geoPostalCodeDescription=""
AE.IP.geoAreaCodeDescription=""
AE.IP.geoTimeZoneDescription="7"
AE.IP.geoLatitudeDescription="13.73417"
AE.IP.geoLongitudeDescription="100.52917"
AE.IP.dmaDescription=""
AE.IP.msaDescription=""
AE.IP.connectionTypeDescription="tx"
AE.IP.lineSpeedDescription="high"
AE.IP.ipRoutingTypeDescription="fixed"
AE.IP.geoAsnDescription="23969"
AE.IP.sldDescription="totbb"
AE.IP.tldDescription="net"
AE.IP.organizationDescription="dynamic ip address for residential broadband customers"
AE.IP.carrierDescription="tot public company limited"
AE.IP.anonymizer_statusDescription="inactive"
AE.IP.proxyLevelDescription="elite"
AE.IP.proxyTypeDescription="http"
AE.IP.proxyLastDetectedDescription="2015-12-22"
AE.IP.hostingFacilityDescription="false"
AE.IP.threatTypeDescription="Anonymous Proxy"
AE.IP.threatCategoryDescription="Anonymous Proxy"
AE.IP.RiskScore="100"
```

Threat types

To determine the type of threat detected, the following table lists the threat types that appear in realm log files.

Threat type risk category definitions

Threat Type (AE.IP.threatType)	Score	SecureAuth IdP Risk Category	Definition
Anonymous Proxy	100	Extreme	Authentication is coming from a server that is designed to hide or anonymize the actual source IP Address

Attacker	99	Extreme	Indicators confirmed to host malicious content, has functioned as a command-and-control (C2) server, and / or has otherwise acted as a source of malicious activity
Compromised	98	Extreme	Indicators confirmed to host malicious content due to compromise or abuse – the exact time and length of compromise is unknown unless disclosed within the report
Related	88	High	Indicators likely related to an attack, but potentially only partially confirmed – detailed by one or more methods, like passive DNS, geo-location, and connectivity detection
Victim	89	High	Indicators representing an entity that has been confirmed to have been victimized by malicious activity, where actors have attempted or succeeded compromise
Uncategorized	80	High	Uncategorized threat
No Threat Found	0	Low	Not found in threat aggregation platform

Threat categories

To determine the category of threat detected, the following table lists the threat categories that appear in realm log files.

Threat category definitions

Threat Category (AE.IP.threatCategory)	Response Value	Definition
Anonymous Proxy	0	Authentication is coming from a server that is designed to hide of anonymize the actual source IP Address
Cyber Espionage	1	Global issue with highly sophisticated nation-states and other actors targeting military, political, and commercial interests to gain decision advantage
Hacktivism	2	Activity ranges from nuisance level to sophisticated campaigns conducted by globally coordinated actors using increasingly sophisticated tools to negatively impact revenue or damage the brand
Enterprise	3	Threats specifically targeted at Enterprise
Critical Infrastructure	4	Threats specifically targeted at Critical Infrastructure
Cyber Crime	5	Threats typically orchestrated by criminal elements for financial benefit
Vulnerability and Exploitation	6	Threats targeting known software vulnerabilities
No Threat Found	999	Not found in threat aggregation platform