Machine entity data - Agent Desktop ThreatMetrix (TMX)

<h2>GUIDE.SUMMARY What There are Machine Detail attributes available to Fraud Teammates through the Machine Entity View in Agent Desktop. This guide will explain what these attributes mean and how to use them </h2><h2>GUIDE.RELATED_LINKS Related articles <ul> Known Good Account Takeover Seller Risk (HRS/CIT) Seller Risk Management </h2><h2>GUIDE.DETAILED_INFORMATION Internal Information Useful acronyms <ul> ISO2 - International Organization for Standardization 2 digit Country Code PPA Partially Provisioned Account TCP Transition Control Protocol TD Mobile: Trust Defender Mobile (agent type will show agent_mobile as the value) UA User Agent VM Virtual Machine   Machine entity guide Use the search box at the top of the table to search by attribute, or click on the column headers to sort. You can also adjust the number of rows that are displayed by using the "show" drop-down menu.   <table border="1" cellpadding="2" cellspacing="0"> <thead> <tr> <th> Attribute name</th> <th> Tab shown</th> <th> Definition</th> <th> Sample values</th> <th> How it can be used during investigation</th> </tr> </thead> <tbody> <tr> <td align="left" valign="top"> Agent Type</td> <td align="left" valign="top"> Machine Entity </td> <td align="left" valign="top"> Channel through which the member

signed into their account.   Browser_computer = desktop/classic web Agent_mobile = Mobile apps Browser_mobile = NOT mobile web but rather when a user is using desktop/classic web and types m.ebay.com in their browser which is a mobile URL.   </td> <td align="left" valign="top"> browser_computer
 browser_mobile
 agent_mobile</td> <td align="left" valign="top"> Use this field to understand the channel through which the user signed into their account and compare to historical sign-in or PPA registration events.</td> </tr> <tr> <td align="left" valign="top"> Browser Language </td> <td align="left" valign="top"> User Activity </td> <td align="left" valign="top"> The code for the language that the browser is configured to accept which comes from the HTTP header. Codes and their meaning may be found here: http://4umi.com/web/html/languagecodes.php</td> <td align="left" valign="top"> en-US,en;q=0.5
 de-DE
 zh-CN
 zh-CN,zh;q=0.8
 pt-BR,pt;q=0.8,en-US;q=0.6,en;q=0.4 </td> <td align="left" valign="top">   When browser language anomaly is 'YES' on the user activity screen leverage this field along with the flash language field to identify the discrepancy. Look for the 2 character ISO2 country code in both values. Using the users registered address, site, shipping address as to whether either of the language settings make sense. Use this field in general to compare the 2 character ISO2 country code to the users registered address, site, shipping address as to whether the language setting makes sense.   </td> </tr> <tr> <td align="left" valign="top"> Browser Language Anomaly </td> <td align="left" valign="top"> User Activity </td> <td align="left" valign="top"> Indicates as "Yes" there is an anomaly between the browser_language and flash_lang. This happens when both appear, and none of the browser's preferred languages is the same as the flash_lang.</td> <td align="left" valign="top"> yes
 'blank' = no </td> <td align="left" valign="top"> When browser language anomaly is 'YES' on the user activity screen leverage the browser language and flash language fields to identify the discrepancy. Look for the 2 character

ISO2 country code in both values. Using the users registered address, registered site, or shipping address. </td> </tr> <tr> <td align="left" valign="top"> Browser String Anomaly </td> <td align="left" valign="top"> User Activity</td> <td align="left" valign="top"> Indicates as "Yes "if there is an anomaly in the browser string content. </td> <td align="left" valign="top"> yes
 'blank' = no </td> <td align="left" valign="top"> Web browser sends an identification string to the Web server you are visiting. The Web server can dynamically use this information to customize Web pages based on the browser identification.   A normal browser string will appear as follows: <ul> Mozilla/5.0 (Windows; U; Windows NT 5.1; en-US; rv:1.8.1.3) Gecko/20070309 Firefox/2.0.0.3   An abnormal browser string that will trigger anomaly will appear as follows (highlighted in red): <ul> Opera/9.80 (X11; Linux x86_64) Presto/2.12.388 Version/12.14 A/OQgnInUbaAaomTotDEewRgptWyduUHBrLWIzmeAEj3QWM81TDx3uopWjjI4NWTYsxPt

WJ1rmMMfJ9laeUYhhrriRPz1lp90PI5gf9ALOCH4fNd174EMhj1l3gomrWFe3KPd7Durf8R8
 LPgdDvPRx21tAUKfjyI6K7IwdHxM9cGRUDFZkmuMrV78quZNxQuqu Mozilla/5.0 (Windows NT 6.1; rv:30.0; WUID=fe28ecf4563951263391e23eb8d6082c; WTB=592; WUID=fe28ecf4563951263391e23eb8d6082c; WTB=592; WUID=fe28ecf4563951263391e23eb8d6082c; WTB=592; WUID=fe28ecf4563951263391e23eb8d6082c; WTB=592; WUID=fe28ecf4563951263391   When anomalies are detected it can indicate that a bot/web crawler tools is present and the browser string will have added character strings like the ones highlighted above. Not all of these are malicious. When this is showing 'YES' it should be considered a risk signal but should be combined with other suspect attributes/activities before using to determine fraud activity.
 Here is what the contents mean in a normal browser string (example is from Safari on iPad): <ul> Mozilla/5.0 (iPad; U; CPU OS 3_2_1 like Mac OS X; en-us) AppleWebKit/531.21.10 (KHTML, like Gecko) Mobile/7B405 <ul>

Mozilla/5.0: Previously used to indicate compatibility with the Mozilla rendering engine (iPad; U; CPU OS 3_2_1 like Mac OS X; en-us): Details of the system in which the browser is running AppleWebKit/531.21.10: The platform the browser uses (KHTML, like Gecko): Browser platform details Mobile/7B405: This is used by the browser to indicate specific enhancements that are available directly in the browser or through third parties. An example of this is Microsoft Live Meeting which registers an extension so that the Live Meeting service knows if the software is already installed, which means it can provide a streamlined experience to joining meetings.   </td> </tr> <tr> <td align="left" valign="top"> Cookies Enabled</td> <td align="left" valign="top"> User Activity </td> <td align="left" valign="top"> Yes/No - First party cookies are required by most website login forms and shopping carts in order to function correctly. Please note that this attribute is not relevant for TD Mobile. </td> <td align="left" valign="top"> yes
 'blank' = no </td> <td align="left" valign="top"> Fraudsters tend to disable settings on their device in order to reduce the ability for their device to be properly profiled. This includes flash, javascript, cookies and images. When this is set to 'YES' it should be considered a risk signal but should be combined with other suspect attributes/activity before using to determine fraud activity as there are also legitimate reasons why good people also disable this setting. </td> </tr> <tr> <td align="left" valign="top"> Device Time Zone</td> <td align="left" valign="top"> Machine Entity</td> <td align="left" valign="top"> The offset in minutes from UTC on the device clock (for standard or winter time, where applicable) </td> <td align="left" valign="top"> 60
 -140 </td> <td align="left" valign="top"> Use this in conjunction when the time-zone offset anomaly field is showing 'YES'. If the value in this field is changing frequently or now is showing a value that is not consistent with history it could mean that someone is trying to disguise the time zone on their device to match up to accounts being touched. </td> </tr> <tr> <td align="left" valign="top"> Flash Anomaly</td> <td align="left" valign="top"> User Activity </td> <td align="left"

valign="top"> Indicates as "Yes" if Flash is installed but not enabled. Please note that for TD Mobile this is not gathered by Flash, though the value is the same. </td> <td align="left" valign="top"> yes
 'blank' = no </td> <td align="left" valign="top"> Fraudsters tend to disable settings on their device in order to reduce the ability for their device to be properly profiled. This includes flash, javascript, cookies and images. When this is set to 'YES' it should be considered a risk signal but should be combined with other suspect attributes/activity before using to determine fraud activity as there are also legitimate reasons why good people also disable this setting. </td> </tr> <tr> <td align="left" valign="top"> Flash Enabled</td> <td align="left" valign="top"> User Activity </td> <td align="left" valign="top"> This flag is set based on detection of flash using javascript. TrustDefender Mobile: this attribute should be ignored. </td> <td align="left" valign="top"> yes
 'blank' = no </td> <td align="left" valign="top"> Fraudsters tend to disable settings on their device in order to reduce the ability for their device to be properly profiled. This includes flash, javascript, cookies and images. When this is set to 'blank' it should be considered a risk signal but should be combined with other suspect attributes/activity before using to determine fraud activity as there are also legitimate reasons why good people also disable this setting. </td> </tr> <tr> <td align="left" valign="top"> Flash Language</td> <td align="left" valign="top"> Machine Entity</td> <td align="left" valign="top"> Operating System Update configuration detected on the device. Not in use for TD Mobile 2.3 (ios) and TD Mobile 3.0 (Android) onwards. </td> <td align="left" valign="top"> en </td> <td align="left" valign="top"> When browser language anomaly is 'YES' on the user activity screen leverage this field along with the browser language field to identify the discrepancy. Look for the 2 character ISO2 country code in both values. Using the users registered address, site, shipping address as to whether either of the language settings make sense. </td> </tr> <tr> <td align="left" valign="top"> Flash OS</td> <td align="left" valign="top"> Machine Entity</td> <td align="left" valign="top"> The Operating System as reported by Flash. Not in use for TD

Mobile 2.3 (ios) and TD Mobile 3.0 (Android) onwards. </td> <td align="left" valign="top"> Windows XP </td> <td align="left" valign="top">   Use this field to identify whether the value in this field matches to historical and does not appear to be suspicious. When new trends arise and can be associated with a specific OS for Flash, use this field to see if there is a match to a recently reported/known trend. </td> </tr> <tr> <td align="left" valign="top"> Flash Version</td> <td align="left" valign="top"> Machine Entity</td> <td align="left" valign="top"> The version of Flash installed in the client browser. Not in use for TD Mobile 2.3 (ios) and TD Mobile 3.0 (Android) onwards. </td> <td align="left" valign="top"> 8.3
 WIN 18,0,0,209
 MAC 18,0,0,209 </td> <td align="left" valign="top">   Use this field to identify whether the value in this field matches to historical and does not appear to be suspicious. When new trends arise and can be associated with a specific version of Flash, use this field to see if there is a match to a recently reported/known trend. </td> </tr> <tr> <td align="left" valign="top"> Image Anomaly</td> <td align="left" valign="top"> Machine Entity</td> <td align="left" valign="top"> Indicates as "Yes" if there was an anomaly associated with images loading in the browser. Otherwise this attribute does not appear. </td> <td align="left" valign="top"> yes
 'blank' = no </td> <td align="left" valign="top"> Fraudsters tend to disable settings on their device in order to reduce the ability for their device to be properly profiled. This includes flash, javascript, cookies and images. When this is set to 'YES' it should be considered a risk signal but should be combined with other suspect attributes/activity before using to determine fraud activity as there are also legitimate reasons why good people also disable this setting. </td> </tr> <tr> <td align="left" valign="top"> Images Enabled</td> <td align="left" valign="top"> Machine Entity</td> <td align="left" valign="top"> Detects if images are enabled. Although highly uncommon, sometimes advanced users browse without images turned on in their browser in order to avoid advertisements. More common, however, is to disable images to

avoid web-bugs or other tracking techniques that use images deposited on the machine. Please note that this attribute is not relevant for TD Mobile. TrustDefender Mobile: this attribute should be ignored. </td> <td align="left" valign="top"> yes
 'blank' = no </td> <td align="left" valign="top"> Fraudsters tend to disable settings on their device in order to reduce the ability for their device to be properly profiled. This includes flash, javascript, cookies and images. When this is set to 'blank' it should be considered a risk signal but should be combined with other suspect attributes/activity before using to determine fraud activity as there are also legitimate reasons why good people also disable this setting. </td> </tr> <tr> <td align="left" valign="top"> Javascript Enabled</td> <td align="left" valign="top"> User Activity </td> <td align="left" valign="top"> Indicates if javascript is enabled inside the browser.Please note that this attribute is not relevant for TD Mobile. </td> <td align="left" valign="top"> yes
 'blank' = no </td> <td align="left" valign="top"> Fraudsters tend to disable settings on their device in order to reduce the ability for their device to be properly profiled. This includes flash, javascript, cookies and images. When this is set to 'blank' it should be considered a risk signal but should be combined with other suspect attributes/activity before using to determine fraud activity as there are also legitimate reasons why good people also disable this setting. </td> </tr> <tr> <td align="left" valign="top"> OS Anomaly</td> <td align="left" valign="top"> User Activity </td> <td align="left" valign="top"> Indicates as "Yes" if the operating system of the browser is NOT the same as the operating system as detected by TCP profiling. Otherwise this attribute does not appear. </td> <td align="left" valign="top"> yes
 'blank' = no </td> <td align="left" valign="top"> When OS anomaly is 'YES' then review the reason codes to locate a rule which will indicate the conflict. Examples: Potential VM - UA Win - OS Linux, Potential VM - UA Mac - OS Linux. Compare this to other sign-in events in the user's history to see if this is normal. </td> </tr> <tr> <td align="left" valign="top"> Policy Score</td> <td align="left" valign="top"> User Activity </td> <td align="left" valign="top"> The policy score of the policy which is

calculated based on the sum of the risk weights for each of the rules configured within it. </td> <td align="left" valign="top"> 0
 -100
 30 </td> <td align="left" valign="top"> Score range is from 100 to -100; the higher the negative score the higher risk of the associated sign-in event or PPA registration. </td> </tr> <tr> <td align="left" valign="top"> Profiled Domain</td> <td align="left" valign="top"> User Activity </td> <td align="left" valign="top"> The URL (i.e. domain + path + query string) of the referring page. </td> <td align="left" valign="top"> signin.ebay.com
 signin.ebay.com.au
 com.ebay.mobile (Android)
 signin.ebay.co.uk
 ebay (iPhone) </td> <td align="left" valign="top"> For the desktop/classic web channel each eBay site has its own unique sign-in page which will trigger a unique profiled domain. ebay.com is for US (site 0) and all other sites will have their country abbreviation within it. For mobile apps you will generally see the same shared profiled domain = com.ebay.mobile (Android) for all sites. The profiled domain will allow you to identify which site/channel is being used to access their eBay account and compare it to historical sign-ins to see if out of pattern. </td> </tr> <tr> <td align="left" valign="top"> Proxy IP</td> <td align="left" valign="top"> Machine Entity</td> <td align="left" valign="top"> If available, the IP address of the proxy. </td> <td align="left" valign="top"> 162.213.197.190 </td> <td align="left" valign="top">   Use this field to understand geographically where the customer may be located and whether it appears to be normal based on their sign-in history, registration address, registered site or shipping address. NOTE: If a proxy is detected this will provide the true geo information that was covered up by the user. There are 3 IP addresses collected. Client IP (aka input IP), Proxy IP and True IP. Only when a proxy is detected will the client IP and true IP vary and generally the client IP will always match the proxy IP. Otherwise if no proxy is detected likely all 3 IP fields will have the same values. </td> </tr> <tr> <td align="left" valign="top"> Proxy IP Assertion History</td> <td align="left" valign="top"> Machine Entity</td>

<td align="left" valign="top"> The history for this proxy IP based on the assertions performed. </td> <td align="left" valign="top"> NEGATIVE_HISTORY </td> <td align="left" valign="top"> If 'NEGATIVE_HISTORY' is present this indicates that sometime after the first seen date of IP address someone in the ThreatMetrix global network has flagged this IP address with risky activity. </td> </tr> <tr> <td align="left" valign="top"> Proxy IP City</td> <td align="left" valign="top"> Machine Entity</td> <td align="left" valign="top"> The city the Proxy IP is located in.</td> <td align="left" valign="top"> waikanae</td> <td align="left" valign="top">   Use this field to understand geographically where the customer may be located and whether it appears to be normal based on their sign-in history, registration address, and registered site or shipping address. NOTE: If a proxy is detected this will provide the true geo information that was covered up by the user. There are 3 IP addresses collected. Client IP (aka input IP), Proxy IP and True IP. Only when a proxy is detected will the client IP and true IP vary and generally the client IP will always match the proxy IP. Otherwise if no proxy is detected likely all 3 IP fields will have the same values. </td> </tr> <tr> <td align="left" valign="top"> Proxy IP First Seen</td> <td align="left" valign="top"> Machine Entity</td> <td align="left" valign="top"> The date that this entity was first encountered in yyyy-mm-dd format across TMX global network.</td> <td align="left" valign="top"> Wed Mar 11 17:00:00 GMT-0700 2015</td> <td align="left" valign="top"> This will help you understand when the IP address was first seen across the entire ThreatMetrix global network. If the date is more current its relationship hasn't likely had time to mature and can be considered risky. </td> </tr> <tr> <td align="left" valign="top"> Proxy IP Geo</td> <td align="left" valign="top"> Machine Entity</td> <td align="left" valign="top"> The 2 character ISO2 country code of the proxy ip country: http://www.iso.org/iso/country_codes.</td> <td align="left" valign="top"> NZ</td> <td align="left" valign="top">   Use this field to understand geographically where the customer may be located and whether it appears

to be normal based on their sign-in history, registration address, registered site or shipping address. NOTE: If a proxy is detected this will provide the true geo information that was covered up by the user. There are 3 IP addresses collected. Client IP (aka input IP), Proxy IP and True IP. Only when a proxy is detected will the client IP and true IP vary and generally the client IP will always match the proxy IP. Otherwise if no proxy is detected likely all 3 IP fields will have the same values. </td> </tr> <tr> <td align="left" valign="top"> Proxy IP ISP</td> <td align="left" valign="top"> Machine Entity</td> <td align="left" valign="top"> The ISP that the Proxy IP address originates from. This may not be the same as the actual owner of the IP range with the ISP which can be found separately using the proxy IP organization.</td> <td align="left" valign="top"> incero llc</td> <td align="left" valign="top">   Helpful to use this when the IP address is changing from one sign-in to another however if the organization and/or ISP is consistent looking at other sign-ins historically then it can reduce concerns with fraudulent activity. There are 3 IP addresses collected. Client IP (aka input IP), Proxy IP and True IP. Only when a proxy is detected will the client IP and true IP vary and generally the client IP will always match the proxy IP. Otherwise if no proxy is detected likely all 3 IP fields will have the same values. </td> </tr> <tr> <td align="left" valign="top"> Proxy IP Organization</td> <td align="left" valign="top"> Machine Entity</td> <td align="left" valign="top"> The organization that the proxy IP address originates from. For example: Lowe's may be the organization owner for a certain IP range however the ISP provider is Comcast.</td> <td align="left" valign="top"> incero llc </td> <td align="left" valign="top">   Helpful to use this when the IP address is changing from one sign-in to another however if the organization and/or ISP is consistent looking at other sign-ins historically then it can reduce concerns with fraudulent activity. There are 3 IP addresses collected. Client IP (aka input IP), Proxy IP and True IP. Only when a proxy is detected will the client IP and true IP vary and generally the client IP will always match the proxy IP. Otherwise if no proxy is detected likely all

3 IP fields will have the same values. </td> </tr> <tr> <td align="left" valign="top"> Proxy IP Region</td> <td align="left" valign="top"> Machine Entity</td> <td align="left" valign="top"> The region the Proxy IP is located in.</td> <td align="left" valign="top"> wellington</td> <td align="left" valign="top">   Use this field to understand geographically where the customer may be located and whether it appears to be normal based on their sign-in history, registration address, registered site or shipping address. NOTE: If a proxy is detected this will provide the true geo information that was covered up by the user. There are 3 IP addresses collected. Client IP (aka input IP), Proxy IP and True IP. Only when a proxy is detected will the client IP and true IP vary and generally the client IP will always match the proxy IP. Otherwise if no proxy is detected likely all 3 IP fields will have the same values. </td> </tr> <tr> <td align="left" valign="top"> Proxy Type</td> <td align="left" valign="top"> User Activity </td> <td align="left" valign="top"> Used to classify the type, and hence risk of the proxy in real time No no proxy is detected Hidden proxy is trying to avoid detection. This is the highest risk proxy type. Open proxy is an open proxy Transparent proxy is a transparent proxy</td> <td align="left" valign="top"> transparent
 hidden
 anonymous</td> <td align="left" valign="top"> Fraudsters tend to hide their true IP geo behind a proxy to avoid detection that they are accessing an eBay account that doesn't match up to our customer's geographical location to reduce suspicion. When using a proxy there are different types of proxy connections to use and each one can have a different level of difficulty to pierce through and detect the true IP geo behind it. Transparent = low/medium risk, Anonymous = medium/high risk, Hidden = high risk. If one of these values appear in AD click on the expander option to see the proxy IP attributes. The true IP if it can be detected will also appear in AD on user activity screen and can be used to compare to proxy to rule out suspicion. It is important to know there are valid reasons why good people use proxies as well and therefore if it is commonly seen with the customer's historical sign-ins then less severity should be given to it. </td>

</tr> <tr> <td align="left" valign="top"> Risk Rating</td> <td align="left" valign="top"> User Activity </td> <td align="left" valign="top"> Risk level mapped from the policy score for each event. This is defined by eBay. High = -30 to -100, Medium = -20 to -30, Low = 0 to -10, Neutral = 0, Trusted = +1 to +100.</td> <td align="left" valign="top"> High
 Medium
 Low
 Trusted
 Neutral </td> <td align="left" valign="top"> When the risk rating is medium or high review all of the eBay reason codes that triggered as that is what led to the higher risk rating. Look for known risky reason codes or ones that differ from the customer's normal history and consider as risk signals to be used in final decision of action taken for said account.</td> </tr> <tr> <td align="left" valign="top"> Screen Res Anomaly</td> <td align="left" valign="top"> User Activity </td> <td align="left" valign="top"> Yes only if the screen resolution is not in the list of acceptable screen resolutions.</td> <td align="left" valign="top"> yes
 'blank' = no </td> <td align="left" valign="top"> Use this field to identify whether the value in this field matches to historical and whether is out of pattern. If it is not normal then it should be considered a risk signal however on its own does not necessarily translate to fraud.</td> </tr> <tr> <td align="left" valign="top"> Session Anomaly</td> <td align="left" valign="top"> Machine Entity</td> <td align="left" valign="top"> Indicates as "Yes" if the browser_string_hash or first_party_cookie changes during the session, and also if the TCP profiling detects changes in the operating system. Otherwise this attribute does not appear.</td> <td align="left" valign="top"> yes
 'blank' = no</td> <td align="left" valign="top"> Could indicate possible cookie stealing or remote connection through another device (i.e. virtual machine). If this is anomaly does not normally trigger historically it should be considered a risk signal however on its own does not necessarily translate to fraud. </td> </tr> <tr> <td align="left" valign="top"> Time Zone Offset Anomaly</td> <td align="left" valign="top"> User Activity </td> <td align="left" valign="top"> Yes if the timezone offset is not an official timezone offset in any country.

Customers should use a policy rule to check if the timezone is appropriate for the geographical location of the device (if known).</td> <td align="left" valign="top"> yes
 'blank' = no</td> <td align="left" valign="top"> When time zone offset anomaly is 'YES' then you can look at the current value in the device time zone field and compare that value to historical values to see if the number is much different. If currently different then most sign-in events it could be considered a risk signal however it is possible that the customer is traveling and has temporarily adjusted their time settings on their device. </td> </tr> <tr> <td align="left" valign="top"> True IP</td> <td align="left" valign="top"> Machine Entity</td> <td align="left" valign="top"> The true client IP Address detected by our 3rd party vendor. </td> <td align="left" valign="top"> 204.236.73.181</td> <td align="left" valign="top">   Use this field to understand geographically where the customer may be located and whether it appears to be normal based on their sign-in history, registration address, registered site or shipping address. NOTE: If a proxy is detected this will provide the true geo information that was covered up by the user. There are 3 IP addresses collected. Client IP (aka input IP), Proxy IP and True IP. Only when a proxy is detected will the client IP and true IP vary and generally the client IP will always match the proxy IP. Otherwise if no proxy is detected likely all 3 IP fields will have the same values. </td> </tr> <tr> <td align="left" valign="top"> True IP Assertion History</td> <td align="left" valign="top"> Machine Entity</td> <td align="left" valign="top"> The history for this true IP based on the assertions performed.</td> <td align="left" valign="top"> NEGATIVE_HISTORY</td> <td align="left" valign="top"> If 'NEGATIVE_HISTORY' is present this indicates that sometime after the first seen date of IP address someone in the ThreatMetrix global network has flagged this IP address with risky activity. </td> </tr> <tr> <td align="left" valign="top"> True IP City</td> <td align="left" valign="top"> Machine Entity</td> <td align="left" valign="top"> The city that the True IP is located in.</td> <td align="left" valign="top"> fremont</td> <td

align="left" valign="top">   Use this field to understand geographically where the customer may be located and whether it appears to be normal based on their sign-in history, registration address, registered site or shipping address. NOTE: If a proxy is detected this will provide the true geo information that was covered up by the user. There are 3 IP addresses collected. Client IP (aka input IP), Proxy IP and True IP. Only when a proxy is detected will the client IP and true IP vary and generally the client IP will always match the proxy IP. Otherwise if no proxy is detected likely all 3 IP fields will have the same values. </td> </tr> <tr> <td align="left" valign="top"> True IP First Seen</td> <td align="left" valign="top"> Machine Entity</td> <td align="left" valign="top"> The date that this entity was first encountered in yyyy-mm-dd format across TMX global network.</td> <td align="left" valign="top"> Mon Mar 4 16:00:00 GMT-0800 2013 </td> <td align="left" valign="top"> This will help you understand when the IP address was first seen across the entire ThreatMetrix global network. If the date is more current its relationship hasn't likely had time to mature and can be considered risky. </td> </tr> <tr> <td align="left" valign="top"> True IP Geo</td> <td align="left" valign="top"> User Activity / Machine Entity</td> <td align="left" valign="top"> The 2 character ISO2 country code of the True IP Address.</td> <td align="left" valign="top"> US
 DE</td> <td align="left" valign="top">   Use this field to understand geographically where the customer may be located and whether it appears to be normal based on their sign-in history, registration address, registered site or shipping address. NOTE: If a proxy is detected this will provide the true geo information that was covered up by the user. There are 3 IP addresses collected. Client IP (aka input IP), Proxy IP and True IP. Only when a proxy is detected will the client IP and true IP vary and generally the client IP will always match the proxy IP. Otherwise if no proxy is detected likely all 3 IP fields will have the same values. </td> </tr> <tr> <td align="left" valign="top"> True IP ISP</td> <td align="left" valign="top"> User Activity / Machine Entity</td> <td align="left" valign="top"> The ISP that the True IP

address originates from. This may not be the same as the actual owner of the IP range with the ISP which can be found separately using the true IP organization.</td> <td align="left" valign="top"> hurricane electric inc.</td> <td align="left" valign="top">   Helpful to use this when the IP address is changing from one sign-in to another however if the organization and/or ISP is consistent looking at other sign-ins historically then it can reduce concerns with fraudulent activity. There are 3 IP addresses collected. Client IP (aka input IP), Proxy IP and True IP. Only when a proxy is detected will the client IP and true IP vary and generally the client IP will always match the proxy IP. Otherwise if no proxy is detected likely all 3 IP fields will have the same values. </td> </tr> <tr> <td align="left" valign="top"> True IP Organization</td> <td align="left" valign="top"> Machine Entity</td> <td align="left" valign="top"> The organization that the True IP address originates from. For example: Lowe's may be the organization owner for a certain IP range however the ISP provider is Comcast.</td> <td align="left" valign="top"> cantv servicios venezuela</td> <td align="left" valign="top">   Helpful to use this when the IP address is changing from one sign-in to another however if the organization and/or ISP is consistent looking at other sign-ins historically then it can reduce concerns with fraudulent activity.   There are 3 IP addresses collected. Client IP (aka input IP), Proxy IP and True IP. Only when a proxy is detected will the client IP and true IP vary and generally the client IP will always match the proxy IP. Otherwise if no proxy is detected likely all 3 IP fields will have the same values. </td> </tr> <tr> <td align="left" valign="top"> True IP Region</td> <td align="left" valign="top"> User Activity / Machine Entity </td> <td align="left" valign="top"> The state/region the True Ip originates from.</td> <td align="left" valign="top"> oregon
 bacau</td> <td align="left" valign="top">   Use this field to understand geographically where the customer may be located and whether it appears to be normal based on their sign-in history, registration address, and registered site or shipping address. NOTE: If a proxy is detected this will provide the

true geo information that was covered up by the user. There are 3 IP addresses collected. Client IP (aka input IP), Proxy IP and True IP. Only when a proxy is detected will the client IP and true IP vary and generally the client IP will always match the proxy IP. Otherwise if no proxy is detected likely all 3 IP fields will have the same values. </td> </tr> <tr> <td align="left" valign="top"> UA Browser</td> <td align="left" valign="top"> Machine Entity</td> <td align="left" valign="top"> The browser type, parsed from the http user agent / "browser" string. User agent is software that is acting on behalf of a user. A user agent string captures which browser you are using, its version number, operating system and its version.</td> <td align="left" valign="top"> chrome 44.0
 firefox 39.0
 ie 9.0
 MSIE 10
 Safari </td> <td align="left" valign="top">   Use this field to compare current activity in question to historical sign-in or PPA registration events to determine if use of browser is consistent. When new trends arise and can be associated with a specific UA browser, use this field to see if there is a match to a recently reported/known trend. </td> </tr> <tr> <td align="left" valign="top"> UA OS</td> <td align="left" valign="top"> Machine Entity</td> <td align="left" valign="top"> The operating system type, parsed from the http user agent / "browser" string. User agent is software that is acting on behalf of a user. A user agent string captures which browser you are using, its version number, operating system and its version.</td> <td align="left" valign="top"> Android
 win8.1
 linux
 iOS
 'blank' = gaming console</td> <td align="left" valign="top">   Use this field to compare current activity in question to historical sign-in or PPA registration events to determine if use of UA OS is consistent. When new trends arise and can be associated with a specific UA OS, use this field to see if there is a match to a recently reported/known trend. </td> </tr> <tr> <td align="left" valign="top"> OS</td> <td align="left" valign="top"> Machine Entity</td> <td align="left" valign="top"> Operating system as indicated by the client browser or mobile library.</td> <td align="left"

valign="top"> Intel Mac OS X
 Linux x86_64
 Windows NT
 Windows NT 5.1
 iPhone OS
 'blank' = Android mobile or gaming console</td> <td align="left" valign="top">   Use this field to compare current activity in question to historical sign-in or PPA registration events to determine if use of OS is consistent. When new trends arise and can be associated with a specific OS, use this field to see if there is a match to a recently reported/known trend. </td> </tr> <tr> <td align="left" valign="top"> TMX Summary Reason Code</td> <td align="left" valign="top"> Machine Entity</td> <td align="left" valign="top"> Summarizes the various rule fires created by TMX. The summary reason code is used for the easy identification of a set of rules by using a common summary field for them.</td> <td align="left" valign="top"> Device_Negative_History
 IP_Negative_History
 IP_Spoofing
 GEO_Spoofing
 Bot</td> <td align="left" valign="top"> Use these different reason codes that triggered to understand a pattern of activity that is being highlighted as part of a related sign-in or PPA registration event just as a teammate would for using the related works tab to see LVIS rule fires. </td> </tr> <tr> <td align="left" valign="top"> eBay Reason Code</td> <td align="left" valign="top"> Machine Entity</td> <td align="left" valign="top"> The names of rules created by eBay that have triggered for a sign-in or PPA registration.</td> <td align="left" valign="top"> 10Accounts1ExactIDin1DMobile
 Accountto3TrueIPinDay</td> <td align="left" valign="top"> Use these different reason codes that triggered to understand a pattern of activity that is being highlighted as part of a related sign-in or PPA registration event just as a teammate would for using the related works tab to see LVIS rule fires. </td> </tr> <tr> <td align="left" valign="top"> Unique IP (input IP) - RENAME TO CLIENT IP </td> <td align="left" valign="top"> User Activity</td> <td align="left" valign="top"> IP address as detected by web server. </td> <td align="left" valign="top"> 204.236.73.181</td> <td align="left" valign="top">   Use this field to understand geographically where the customer may be located and

whether it appears to be normal based on their sign-in history, registration address, and registered site or shipping address. There are 3 IP addresses collected. Client IP (aka input IP), Proxy IP and True IP. Only when a proxy is detected will the client IP and true IP vary and generally the client IP will always match the proxy IP. Otherwise if no proxy is detected likely all 3 IP fields will have the same values </td> </tr> <tr> <td align="left" valign="top"> IP City - RENAME TO CLIENT IP CITY</td> <td align="left" valign="top"> User Activity</td> <td align="left" valign="top"> The city the Input IP Address is located in</td> <td align="left" valign="top"> fremont</td> <td align="left" valign="top">   Use this field to understand geographically where the customer may be located and whether it appears to be normal based on their sign-in history, registration address, and registered site or shipping address. There are 3 IP addresses collected. Client IP (aka input IP), Proxy IP and True IP. Only when a proxy is detected will the client IP and true IP vary and generally the client IP will always match the proxy IP. Otherwise if no proxy is detected likely all 3 IP fields will have the same values </td> </tr> <tr> <td align="left" valign="top"> IP Country - RENAME TO CLIENT IP GEO</td> <td align="left" valign="top"> User Activity</td> <td align="left" valign="top"> The 2 character ISO2 country code of the Input IP Address.</td> <td align="left" valign="top"> CN</td> <td align="left" valign="top">   Use this field to understand geographically where the customer may be located and whether it appears to be normal based on their sign-in history, registration address, and registered site or shipping address. There are 3 IP addresses collected. Client IP (aka input IP), Proxy IP and True IP. Only when a proxy is detected will the client IP and true IP vary and generally the client IP will always match the proxy IP. Otherwise if no proxy is detected likely all 3 IP fields will have the same values </td> </tr> <tr> <td align="left" valign="top"> ADD - CLIENT IP REGION</td> <td align="left" valign="top"> User Activity</td> <td align="left" valign="top"> The region the Input IP Address is located in</td> <td align="left" valign="top">

oregon
 bacau</td> <td align="left" valign="top">   Use this field to understand geographically where the customer may be located and whether it appears to be normal based on their sign-in history, registration address, and registered site or shipping address. There are 3 IP addresses collected. Client IP (aka input IP), Proxy IP and True IP. Only when a proxy is detected will the client IP and true IP vary and generally the client IP will always match the proxy IP. Otherwise if no proxy is detected likely all 3 IP fields will have the same values </td> </tr> <tr> <td align="left" valign="top"> ADD - CLIENT IP ISP</td> <td align="left" valign="top"> User Activity</td> <td align="left" valign="top"> The ISP that the Input IP address originates from.</td> <td align="left" valign="top"> hurricane electric inc.</td> <td align="left" valign="top">   Helpful to use this when the IP address is changing from one sign-in to another however if the organization and/or ISP is consistent looking at other sign-ins historically then it can reduce concerns with fraudulent activity.   There are 3 IP addresses collected. Client IP (aka input IP), Proxy IP and True IP. Only when a proxy is detected will the client IP and true IP vary and generally the client IP will always match the proxy IP. Otherwise if no proxy is detected likely all 3 IP fields will have the same values </td> </tr> <tr> <td align="left" valign="top"> ADD - CLIENT IP ORGANIZATION</td> <td align="left" valign="top"> User Activity</td> <td align="left" valign="top"> The organization that the Input IP address originates from</td> <td align="left" valign="top"> cantv servicios venezuela</td> <td align="left" valign="top">   Helpful to use this when the IP address is changing from one sign-in to another however if the organization and/or ISP is consistent looking at other sign-ins historically then it can reduce concerns with fraudulent activity.   There are 3 IP addresses collected. Client IP (aka input IP), Proxy IP and True IP. Only when a proxy is detected will the client IP and true IP vary, and generally the client IP will always match the proxy IP. Otherwise if no proxy is detected likely all 3 IP fields will have the same values </td> </tr> <tr> <td

align="left" valign="top"> Exact ID</td> <td align="left" valign="top"> Machine Entity</td> <td align="left" valign="top"> SmartID is cookieless, and is based exclusively on device attribute to improve detection of returning visitors, especially those trying to elude identification, and reduces false positives. Note that the associated attribute entities are named as follows: fuzzy_device (omitting the 'id')</td> <td align="left" valign="top"> 92c31153e4324ac28c0ef3d7c828ddec</td> <td align="left" valign="top"> Use this field to compare current activity in question to historical sign-in or PPA registration events to determine if the device has been seen before or is consistent. This individual device identifier is mapped to MGID's which is what teammates have traditionally seen as the device ID in CS tools. </td> </tr> <tr> <td align="left" valign="top"> Smart ID</td> <td align="left" valign="top"> Machine Entity</td> <td align="left" valign="top"> ExactID is a persistent global identifier which relies on a variety of persistent markers (browser cookies, Adobe Flash cookies, HTML 5 local storage) to allow ThreatMetrix to 100% accurately identify a device. Note that the related entity attributes are named device_ (excluding the 'id' from the attribute names)</td> <td align="left" valign="top"> 06b240dd9861438db590d26615aa854f</td> <td align="left" valign="top"> Use this field to compare current activity in question to historical sign-in or PPA registration events to determine if the device has been seen before or is consistent. This individual device identifier is mapped to MGID's which is what teammates have traditionally seen as the device ID in CS tools. </td> </tr> </tbody> </table>   </h2>