CyberSource Decision Manager

Device Fingerprinting Guide

September 2014

CyberSource®
the power of payment

CyberSource Corporation HQ | P.O. Box 8999 | San Francisco, CA 94128-8999 | Phone: 800-530-9095

CyberSource Contact Information

For general information about our company, products, and services, go to http://www.cybersource.com.

For sales questions about any CyberSource Service, email sales@cybersource.com or call 650-432-7350 or 888-330-2300 (toll free in the United States).

For support information about any CyberSource Service, visit the Support Center at http://www.cybersource.com/support.

Copyright

Restricted Rights Legends

Trademarks

Contents

Recent Revisions to This Document

Release	Changes
September 2014	Enhanced the description of Smart IDs. See "Smart IDs," page 12.
July 2014	Added information about the new **deviceFingerprintHash** Simple Order API request field and the new **device_fingerprint_hash** SCMP API request field. See the Simple Order API "Request Fields," page 42, or the SCMP API "Request Fields," page 52, depending on the API version you are using.
June 2014	■ Corrected name of the class in the mobile SDK that is used for device fingerprint implementations in Android and iOS applications. See "Implementing the Device Fingerprinting SDK in Android Applications," page 18, and "Implementing the Device Fingerprinting SDK in iOS Applications," page 20. ■ Added additional explanatory comment to the beginning of the "Android Code Example," page 19.
May 2014	■ Added information about implementing the new Device Fingerprinting mobile SDK. See "Mobile Implementations," page 18. ■ Added the following new Simple Order API reply fields. See the Simple Order API "Reply Fields," page 43. • afsReply_deviceFingerprint_agentType • afsReply_deviceFingerprint_dateTime • afsReply_deviceFingerprint_deviceLatitude (mobile only) • afsReply_deviceFingerprint_deviceLongitude (mobile only) • afsReply_deviceFingerprint_deviceMatch • afsReply_deviceFingerprint_firstEncounter • afsReply_deviceFingerprint_flashOS • afsReply_deviceFingerprint_flashVersion • afsReply_deviceFingerprint_gpsAccuracy(mobile only) • afsReply_deviceFingerprint_jbRoot (mobile only) • afsReply_deviceFingerprint_jbRootReason (mobile only) • afsReply_deviceFingerprint_profileDuration • afsReply_deviceFingerprint_profiledURL • afsReply_deviceFingerprint_timeOnPage

Release	Changes
May 2014	■ Added the following new SCMP API reply fields. See the SCMP API "Reply Fields," page 53. • score_device_fingerprint_agent_type • score_device_fingerprint_date_time • score_device_fingerprint_device_latitude (mobile only) • score_device_fingerprint_device_longitude (mobile only) • score_device_fingerprint_device_match • score_device_fingerprint_first_encounter • score_device_fingerprint_flash_os • score_device_fingerprint_flash_version • score_device_fingerprint_gps_accuracy (mobile only) • score_device_fingerprint_jb_root (mobile only) • score_device_fingerprint_jb_root_reason (mobile only) • score_device_fingerprint_profile_duration • score_device_fingerprint_profiled_url • score_device_fingerprint_time_on_page ■ Added the following 4 new suspicious data info codes. See "Suspicious Data Information Codes," page 61. • ANOM-BSTR • ANOM-SESS • ANOM-SRAT • ANOM-SRES ■ Added information about new fingerprint fields that are added as Order Elements to the Rule Editor. See "Device Fingerprinting Order Elements," page 26. ■ Added the following 15 new fields that appear in the Device Fingerprint details dialog box in the Case Management Details window. See "Device Fingerprint Details," page 36. • Profiling Date/Time • Profiling Duration • Profiled URL • Date Device First Seen • Device Matched • Application Type • Time on Page • Browser Session ID • Flash Operating System • Flash Version • GPS Accuracy • Device Latitude • Device Longitude • Jailbreak/Root Privileges • Jailbreak/Root Reason
February 2014	Increased all API reply fields of the String data type to a length of 255 characters. See Appendix A, "API Fields and Information Codes," on page 42.

About This Guide

Audience and Purpose

This guide describes how to implement *device fingerprinting* on your web site or in your mobile applications. Device fingerprinting is a method of collecting sets of unique and non-unique identifiers that enable you to detect identity morphing, the true location of a device, and the browsing habits of individuals.

The audience for this guide includes:

- Web developers and mobile application developers who modify the check-out page of your company's web site or who develop mobile applications that your customers use to purchase merchandise from you on their phones or tablets.
- Web administrators who manage the web server.
- Software developers who add API fields to transaction requests and replies and who write the software code that integrates CyberSource services with your company's order management system.
- Decision Manager administrators or case management administrators who are responsible for creating Decision Manager profiles and rules that use device fingerprints and Smart IDs to filter transactions.
- Case reviewers who use Decision Manager to review orders. Reviewers can search on device fingerprints to obtain more information about a customer's identity and the device that they used to place their order.

Scope

This guide narrowly focuses on implementing and using device fingerprints and Smart IDs. For information about implementing other CyberSource services and information about using Decision Manager in the Business Center, see "Related Documents," page 10.

Conventions

Note, Important, and Warning Statements

Note

A *Note* contains helpful suggestions or references to material not contained in the document.

Important

An *Important* statement contains information essential to successfully completing a task or learning a concept.

Warning

A *Warning* contains information or instructions, which, if not heeded, can result in a security risk, irreversible loss of data, or significant cost in time or revenue or both.

Text and Command Conventions

Convention	Usage
bold	■ Field and service names in text. For example: Include the **ics_applications** field. ■ Items that you are instructed to act upon. For example: Click **Save**.
italic	■ Filenames and pathnames. For example: Add the filter definition and mapping to your *web.xml* file. ■ Placeholder variables for which you supply particular values.
`monospace`	■ XML elements. ■ Code examples and samples. ■ Text that you enter in an API environment. For example: Set the **davService_run** field to `true`.

Related Documents

- *Decision Manager Developer Guide Using the Simple Order API* describes how to integrate Decision Manager, a fraud detection service, with your order management system by using the Simple Order API. (PDF | HTML)
- *Decision Manager Developer Guide Using the SCMP API* describes how to integrate Decision Manager, a fraud detection service, with your order management system by using the SCMP API. (PDF | HTML)

Note The SCMP API is a legacy name-value pair API that is supported for merchants who have already implemented it. If you are new to CyberSource and want to connect to services, use the Simple Order API.

- *Decision Manager User Guide* describes how to use Decision Manager in the Business Center. (PDF | HTML)
- *Decision Manager Score Builder Guide* describes how to configure custom profile scores to support your business requirements. (PDF | HTML)

Refer to the Support Center for complete CyberSource technical documentation:

http://www.cybersource.com/support_center/support_documentation

Customer Support

For support information about any CyberSource service, visit the Support Center at:

http://www.cybersource.com/support

CHAPTER 1

Implementing Device Fingerprinting

Introduction to Device Fingerprinting

CyberSource Decision Manager Device Fingerprinting gathers information about the devices that are used to place orders on your web site or about devices that use your mobile application. This information gathering is called *device profiling*.

Elements of Device Fingerprinting

Device Fingerprints

The device fingerprint is a unique set of identifiers derived from persistent cookies set during device profiling. This device identifier can be the single constant element that you use to detect identity morphing and the true location of a device. When identity morphing occurs, customer and order data of transactions may appear to be random and derived from different customers, but the device fingerprint does not change. This fingerprint indicates that the transactions originate from a single device.

Fingerprints enable you to identify many characteristics of a device, for example:

- Connections between accounts and other customer data
- True locations of devices when they are hidden behind a proxy
- Suspicious configurations of devices, such as language settings inconsistent with the country

Smart IDs

Unlike device fingerprints, Smart IDs are not based on cookies. They are useful for detecting the browsing patterns of customers who delete cookies, use private browsing mode, or steal cookies from other users. Because of the attributes that are used to create Smart IDs, in rare situations it is possible for two devices, especially mobile devices, to appear with the same Smart ID. Smart IDs have a lifetime of approximately two weeks starting from the first time a device visits a tagged web page or mobile application.

For example, if a device with Smart ID 987654ABC visits a tagged web site once, but does not visit a tagged web site again for 3 weeks, when the device visits a tagged web site again, a *new* Smart ID is assigned to it. However, if that device visits a tagged web site one day, and then visits another tagged web site or the same tagged web site within approximately 14 days, that Smart ID might persist for approximately 14 days more and so on. As long as the device user remains active on tagged pages without lapses that exceed the Smart ID's lifetime, the Smart ID persists and is extended each time the customer visits a tagged page.

How Device Fingerprinting Works

1. Depending on where you are implementing device fingerprinting, you add the device fingerprinting tags to your web site or you add the device fingerprinting code and libraries to your mobile application.

2. When a customer loads your web site into their browser or launches your mobile application, various options and properties are sent to the device fingerprinting server.

3. The device fingerprinting server profiles the device. This profiling process collects device identification information.

4. The device fingerprint ID API field, which contains the same session ID value that is assigned to the transaction by the code that you include on your web site or in your mobile application, is included in your CyberSource request. If you use the Simple Order API, see deviceFingerprintID, page 43. If you use the SCMP API, see device_fingerprint_id, page 52.

5. Depending on what the server detects on the device, the server returns information to Decision Manager about your customers' devices and the session. You can use this information to determine whether the transaction is legitimate or fraudulent.

Notice to European Union Merchants

The European Union's Privacy and Electronic Communications Directive (the “Directive”) restricts the deposit and storage of cookies on the devices of customers of online merchants operating in the European Union.

The device fingerprint feature of CyberSource Decision Manager is one of more than two hundred global fraud detectors and tests. This feature enables the deposit and storage on the customer's computer of a cookie that profiles the specific attributes of the computer used in transactions. This cookie is used to mitigate fraud.

While we cannot provide legal advice to our merchants, we can provide the following information. The restrictions under the Directive require, among other things, that you

- Provide "clear and comprehensive information" to visitors of your web site about the storage of cookies on their computer.
- Obtain the consent of visitors before depositing and storing cookies on their computer unless certain exceptions apply.

Your compliance with applicable privacy laws depends on how you use the cookies, on what information you disclose to customers, and on what consent you obtain from customers. Because CyberSource has no direct connection to your customers, you are responsible for ensuring that cookies are used properly to perform the requested CyberSource services. CyberSource believes that the safest course of action is for you to clearly and conspicuously disclose the use of cookies to your customers and to obtain their consent before placing cookies on their devices. If you operate in Europe and use the device fingerprint, you should consult your legal counsel and other advisors to find out how to comply with the requirements of the Directive and whether an exception might be available for you. CyberSource cannot take any position on the storage of cookies on the devices of customers for purposes other than to provide CyberSource services. When used without the device fingerprint, Decision Manager does not store cookies.

Web Site Implementations

You must configure both your web site and your web server.

Important To ensure your customers' privacy, CyberSource encodes fingerprints as soon as they are received. Add the fingerprint to your request as soon as possible because the fingerprint persists for approximately 30 minutes after it is generated. This interval begins when the customer sees the HTML page with the tags, and it ends when the transaction request is sent to CyberSource.

Warning CyberSource recommends that you use domain names instead of using IP addresses and relying on domain name resolution. If you use an IP address, device fingerprinting stops working if the IP address of the domain name changes.

Adding the Fingerprinting Code to Your Web Site

You must add a 1-pixel image, which is not displayed, and two code segments to the `<body>` tag of your checkout page. To give device profiling time to complete, ensure that 3 to 5 seconds elapse between the execution of the profiling code and when your customers submit their orders.

Warning If you do not add all three code elements to your checkout page, complete and accurate results are not returned.

To add the device fingerprinting code to your web site:

Step 1 Add the One-Pixel Image Code, Flash Code, and JavaScript Code to your checkout page immediately above the closing `</body>` tag to ensure that web pages render correctly. Do not enclose the segments in visible HTML elements. The code segments must be loaded before the customer submits an order. Otherwise, you receive an error message.

Step 2 Replace the variables with your values:

- Domain:
  - For testing:

    Use `h.online-metrix.net`, which is the DNS name of the fingerprint server as shown in the sample HTML tags below.

  - For production:

Change the domain name to a local URL, and configure your web server to redirect the URL to `h.online-metrix.net`.

- ***<org ID>***: To obtain this value, contact your CyberSource representative and specify to them whether it is for testing or production.
- ***<merchant ID>***: Your unique CyberSource merchant ID.
- ***<session ID>***: The session ID is a string variable that must be unique for each transaction. You can use any string that you are already generating, such as an order number or web session ID. However, do not use the same uppercase and lowercase letters to indicate different session IDs. For information about what characters can be used in this field, see the Simple Order API field description of deviceFingerprintID, page 43, or the SCMP API field description of device_fingerprint_id, page 52.

Be sure to copy all characters correctly and to omit the angle brackets (< >) when substituting your values for the variables.

When you have added the code to your web site and tested it, you must configure your web server. See "Configuring Your Web Server," page 17.

One-Pixel Image Code

```
<p style="background:url(https://h.online-metrix.net/fp/
clear.png?org_id=<org ID>&amp;session_id=<merchant id><session
ID>&amp;m=1)"></p>
<img src="https://h.online-metrix.net/fp/clear.png?org_id=<org
ID>&amp;session_id=<merchant id><session ID>&amp;m=2" alt="">
```

Example:

```
<p style="background:url(https://h.online-metrix.net/fp/clear.png?org_
id=sample_orgID&amp;session_id=sample_merchantIDsample_
sessionID&amp;m=1)"></p>
<img src="https://h.online-metrix.net/fp/clear.png?org_id=sample_
orgID&amp;session_id=sample_merchantIDsample_sessionID&amp;m=2" alt="">
```

Flash Code

```
<object type="application/x-shockwave-flash" data="https://h.online-
metrix.net/fp/fp.swf?org_id=<org ID>&amp;session_id=<merchant
id><session ID>" width="1" height="1" id="thm_fp">
<param name="movie" value="https://h.online-metrix.net/fp/fp.swf?org_
id=<org ID>&amp;session_id=<merchant id><session ID>" />
<div></div>
</object>
```

Example:

```
<object type="application/x-shockwave-flash" data="https://h.online-
metrix.net/fp/fp.swf?org_id=sample_orgID&amp;session_id=sample_
merchantIDsample_sessionID" width="1" height="1" id="thm_fp">
<param name="movie" value="https://h.online-metrix.net/fp/fp.swf?org_
id=sample_orgID&amp;session_id=sample_merchantIDsample_sessionID" />
<div></div>
</object>
```

JavaScript Code

```
<script src="https://h.online-metrix.net/fp/check.js?org_id=<org
ID>&amp;session_id=<merchant id><session ID>" type="text/javascript">
</script>
```

Example:

```
<script src="https://h.online-metrix.net/fp/check.js?org_id=sample_
orgID&amp;session_id=sample_merchantIDsample_sessionID" type="text/
javascript">
</script>
```

Configuring Your Web Server

Important If you do not complete this section, the domain name of the third party is visible in the browser address bar, which might cause customers to block it.

All variables listed in Step 2 of "Adding the Fingerprinting Code to Your Web Site," page 14, refer to `h.online-metrix.net`, which is the DNS name of the fingerprint server. When you are ready for production, you must change the server name to a local URL and configure your web server to redirect the URL to `h.online-metrix.net`. For information on redirecting the URL, see your web administrator and the documentation for your web server.

After you have added the code to your web page and configured your web server, you must add the device fingerprinting API field to the API request that you send to CyberSource. See "Specifying the Session ID in CyberSource API Requests," page 23.

Mobile Implementations

You can deploy Decision Manager Device Fingerprinting in Android and iOS applications.

Implementing the Device Fingerprinting SDK in Android Applications

To implement device fingerprinting in Android applications:

Step 1 Download the *CyberSourceTMDeviceFingerprintingMobileSDK_for_Android.zip* file from the Business Center Documentation page, and add it to your project.

Step 2 Include the following permission in the mobile application manifest file:

```
<uses-permission android:name="android.permission.INTERNET">
</uses-permission>
```

Step 3 Specify your merchant ID and the session ID as a concatenated value for a variable that is passed to the `TrustDefenderMobile` class in your Android application. In the following example ***my_variable*** = your merchant ID + the session ID as a concatenated value:

```
profile.setSessionID ("my_variable");
```

The `TrustDefenderMobile` class is contained in the *CyberSourceTMDeviceFingerprintingMobileSDK_for_Android.zip* file. A session ID must be a unique identifier for the transaction, such as an order number. It is a string that can contain lowercase and uppercase English letters, digits, hyphens (-), and underscores (_). The maximum length is 88 characters. For more information, see the Simple Order API request field description of deviceFingerprintID, page 43, or the SCMP API request field description of device_fingerprint_id, page 52.

Step 4 Add the `doProfileRequest()` function to your application, and specify the following required calling options:

Option	Description
Org ID	Contact CyberSource Customer Support for this value and specify whether it is for testing or production.
Fingerprint server URL	h.online-metrix.net

See "Android Code Example," page 19. After you have added the device fingerprinting SDK to your application, you must add the device fingerprinting API field to the API request that you send to CyberSource. See "Specifying the Session ID in CyberSource API Requests," page 23.

Android Code Example

The following excerpt from an Android application shows how to set the `doProfileRequest()` function calling options.

```
//Import the following from your Android package and the
//CyberSourceTMDeviceFingerprintingMobileSDK_for_Android package.
import android.annotation.SuppressLint;
import android.app.Activity;
import android.location.Criteria;
import android.location.Location;
import android.util.Log;
import com.threatmetrix.TrustDefenderMobile.ProfileNotifyV2;
import com.threatmetrix.TrustDefenderMobile.TrustDefenderMobile;
.
.
.

//In the following example, a “profile” variable has been set:
//final TrustDefenderMobile profile = new TrustDefenderMobile();

//Create the profiling request.

void doProfile()

{
   //Assign a session ID for the profiling attempt. The session ID must be a unique
   //value for each transaction. For example, an order number. Then create a variable
   //that concatenates your merchant ID with the session ID. The merchant ID must be
   //the first characters in this variable string. In the following code,
   //my_variable = your merchant ID + the session ID as a concatenated value.

   this.profile.setSessionID(“my_variable”);

   //Send the profiling request. Contact CyberSource Support for your Org ID.

   TrustDefenderMobile.THMStatusCode
   status=this.profile.doProfileRequest(this.getApplicationContext(),”my_orgID”,
   “h.online-metrix.net”);

   if(status == TrustDefenderMobile.THMStatusCode.THM_OK)
   {
      //The profiling successfully started; if a session ID was generated by the SDK,
      //it is available.

      Log.d(“Sample”, “My session ID is “ + this.profile.getSessionID());

   }

}
```

Implementing the Device Fingerprinting SDK in iOS Applications

To implement device fingerprinting in iOS applications:

To develop iOS applications, you must be enrolled in the iOS Developer Program, which enables you to upload your applications to the Apple App Store. To link against the Cybersource device fingerprinting mobile SDK, you must use the iOS 7 SDK or later and the Apple Xcode 5 IDE.

Step 1 Download the *CyberSourceTMDeviceFingerprintingMobileSDK_for_iOS.zip* file and header file from the Business Center Documentation page. You must add both of these to your iOS application project.

Step 2 Import the device fingerprinting SDK libraries and frameworks into your iOS application:

```
#import <TrustDefenderMobile/TrustDefenderMobile.h>
```

For information about linking to libraries and frameworks in iOS applications, see:

https://developer.apple.com/library/ios/recipes/xcode_help-project_editor/Articles/AddingaLibrarytoaTarget.html

Step 3 Link the following frameworks:

- Security
- UIKit
- Foundation
- CoreTelephony
- CoreLocation

Step 4 Specify your merchant ID and the session ID as a concatenated value for a variable that is passed to the `TrustDefenderMobile` class in your iOS application. In the following example ***my_variable*** = your merchant ID + the session ID as a concatenated value:

```
self.profile.sessionID = @"my_variable";
```

The `TrustDefenderMobile` class is contained in the *CyberSourceTMDeviceFingerprintingMobileSDK_for_iOS.zip* file. A session ID must be a unique identifier for the transaction, such as an order number. It is a string that can contain lowercase and uppercase English letters, digits, hyphens (-), and underscores (_). The maximum length is 88 characters. For more information, see the Simple Order API request field description of deviceFingerprintID, page 43, or the SCMP API request field description of device_fingerprint_id, page 52.

Step 5 Add the `doProfileRequest()` function to your application, and specify the following calling options:

Option	Description
Org ID	Contact CyberSource Customer Support for this value and specify whether it is for testing or production.
Fingerprint server URL	h.online-metrix.net

See "iOS Code Example," page 22. After you have added the device fingerprinting SDK to your application, you must add the device fingerprinting API field to the API request that you send to CyberSource. See "Specifying the Session ID in CyberSource API Requests," page 23.

iOS Code Example

The following excerpt from an iOS application shows how to set the `doProfileRequest()` function calling options where ***ApplicationName*** is the name of your iOS application:

```
//Import the following from your CyberSourceTMDeviceFingerprintingMobileSDK_for_iOS
//package.

#import <TrustDefenderMobile/TrustDefenderMobile.h>

@interface ApplicationName :NSObject <TrustDefenderMobileDelegate>
@property (readwrite) TrustDefenderMobile* profile;
.
.
.

//Create the profiling request.
-(void)doProfile
{
   //Assign a session ID for the profiling attempt. The session ID must be a unique
   //value for each transaction. For example, an order number. Then create a variable
   //that concatenates your merchant ID with the session ID. The merchant ID must be
   //the first characters in this variable string. In the following code,
   //my_variable = your merchant ID + the session ID as a concatenated value.

   self.profile.sessionID = @”my_variable”;

   //Send the profiling request. Contact CyberSource Support for your Org ID.

   thm_status_code_t status = [self.profile doProfileRequestFor:@”my_orgID”
   connectingTo:@”h.online-metrix.net”];

   if(status == THM_OK)
   {
      //The profiling successfully started; if a session ID was generated by the SDK,
      //it is now available.

      NSLog(@”My session ID is %@”, self.profile.sessionID);
   }
}
@end
```

Specifying the Session ID in CyberSource API Requests

After you add the device fingerprinting code to your web site or mobile application, you must specify the session ID in Decision Manager transactions by using the deviceFingerprintID Simple Order API request field or the device_fingerprint_id SCMP API request field. If you do not include this API request field along with the other API request fields in the transaction request, no device fingerprinting information is returned in the reply.

After you specify the session ID in your API request, you are ready to test your implementation. See "Testing Your Implementation," page 25.

Specifying the session_id Value

The syntax used to specify the `session_id` value for web pages and mobile applications differs from that used with the API field:

- In web pages and mobile applications, use `session_id=<`***merchant id***`><`*session ID*`>` where your merchant ID is concatenated with the session ID.
- In API requests, use the deviceFingerprintID (Simple Order API) or device_fingerprint_id (SCMP API) field to specify the `<`*session ID*`>`.

Simple Order API Request Examples

For more examples, see "Simple Order API Request and Reply Examples," page 51.

Example 1 Simple Order API Name-Value Pair

```
afsService_run=true
<customer's name and billing address fields>
card_accountNumber=4111xxxxxxxx1111
card_cardType=001
card_expirationMonth=12
card_expirationYear=2018
cc_AuthService_run=true
deviceFingerprintID=583412543162831l477
merchantDefinedData_mddField32=126
merchantID=example
merchantReferenceCode=833617922960995060
purchaseTotals_currency=USD
purchaseTotals_grandTotalAmount=30.00
```

Example 2 Simple Order API XML

```
<requestMessage xmlns=”urn:schemas-cybersource-com:transaction-
dataschema_version_number” >
    <merchantID>example</merchantID>
    <merchantReferenceCode>833617922960995060</merchantReferenceCode>
    <billTo>
        <customer’s name and billing address fields>
    </billTo>
    <purchaseTotals>
        <currency>USD</currency>
        <grandTotalAmount>30.00</grandTotalAmount>
    </purchaseTotals>
    <card>
        <accountNumber>4111xxxxxxxx1111</accountNumber>
        <cardType>001</cardType>
        <expirationMonth>12</expirationMonth>
        <expirationYear>2018</expirationYear>
    </card>
    <merchantDefinedData>
        <mddField id=”32”>126</mddField>
    </merchantDefinedData>
    <afsService run=”true”>
    <ccAuthService run=”true”>
    <deviceFingerprintID>5834125431628311477</deviceFingerprintID>
</requestMessage>
```

SCMP API Request Example

Only name-value pairs are supported in the SCMP API. For more examples, see "SCMP API Request and Reply Examples," page 60.

```
ics_applications=ics_score
<customer’s name and billing address fields>
customer_cc_number=4111xxxxxxxx1111
card_type=001
customer_cc_expmo=12
customer_cc_expyr=2018
ics_applications=ics_auth
device_fingerprint_id=5834125431628311477
merchant_defined_data32=126
merchant_id=example
merchant_ref_number=833617922960995060
currency=USD
grand_total_amount=30.00
```

Testing Your Implementation

To test your implementation:

Step 1 Create a custom rule to screen orders for the presence of a fingerprint.

Step 2 Send a test API request. Your test reply contains a fingerprint if your implementation is correct.

CHAPTER 2

Configuring Custom Rules, Lists, and Velocity Rules

You can use the device fingerprinting attributes that are returned in the API reply to configure rules for order profiles.

Device Fingerprinting Order Elements

This table lists device fingerprinting order elements that are available in the Rule Editor:

Table 1 Available Device Fingerprinting Order Elements

- Application type
- Browser language
- Cookies enabled
- Device fingerprint
- Device latitude
- Device longitude
- Device matched
- Flash enabled
- Flash operating system
- Flash version
- GPS accuracy
- Images enabled
- Jailbreak/root privileges
- Jailbreak/root reason
- JavaScript enabled
- Profiling duration
- Profiled URL
- Proxy IP address
- Proxy IP address activities
- Proxy IP address attributes
- Proxy server type
- Screen resolution
- Smart ID
- Smart ID confidence level
- Time on page
- True IP address
- True IP address activities
- True IP address attributes
- True IP address city
- True IP address country

For other order elements that are available in the Rule Editor, see Appendix A “Custom Rules Elements and Examples” in the *Decision Manager User Guide* (PDF | HTML).

Custom Rule Examples

Screening for Suspicious Device Fingerprints

You can create custom rules that specify identity, suspicious, and velocity information codes that can be returned in replies. This example shows a rule to screen orders for the presence of a fingerprint that was already deemed suspicious. If the rule is triggered, the third condition increases the probability that the order is fraudulent. For a complete list of Fraud Score order elements, see Appendix A in the *Decision Manager User Guide* (PDF | HTML).

Example 3 Rule That Screens for Suspicious Device Fingerprint

First condition	
Order element	Fraud score suspicious information
Comparison operator	contains
Comparison values	Devise confirmed risky
Second condition	
Order element	Fraud score customer list information
Comparison operator	contains
Comparison value	Device fingerprint on negative list
Third condition	
Order element	Fraud score suspicious information
Comparison operator	contains
Comparison values	Masked device history
Condition relationship	At least one condition is true.
Profile Setting	Reject orders that contain a true condition.

Screening for Disabled Browser Attributes

This example shows a rule that triggers a review of orders when a customer disables browser attributes that might indicate suspicious activity. This example contains all possible elements that can be detected as disabled in customers' browsers. However, your rule might contain only those that you consider most likely to reveal suspicious activity for your business.

Example 4 Rule That Screens for Disabled Browser Attributes

First condition	
Order element	Cookies enabled
Comparison operator	is equal to
Comparison values	false
Second condition	
Order element	Flash enabled
Comparison operator	is equal to
Comparison value	false
Third condition	
Order element	Images enabled
Comparison operator	is equal to
Comparison values	false
Fourth condition	
Order element	JavaScript enabled
Comparison operator	is equal to
Comparison values	false
Condition relationship	All conditions are true.
Profile setting	Review or reject orders that contain all true conditions.

Screening for Device Type

This example shows a rule that helps you to discover the type of device used to place the order, such as a mobile phone.

Example 5 Rule That Screens for Device Type

First condition	
Order element	Application type
Comparison operator	is equal to
Comparison values	Custom value (for example: `browser_mobile`)
Second condition	
Order element	Device latitude
Comparison operator	is present
Third condition	
Order element	GPS accuracy
Comparison operator	is present
Condition relationship	At least one condition is true.
Profile setting	Review orders that trigger the rule.

Screening for IP Address Characteristics

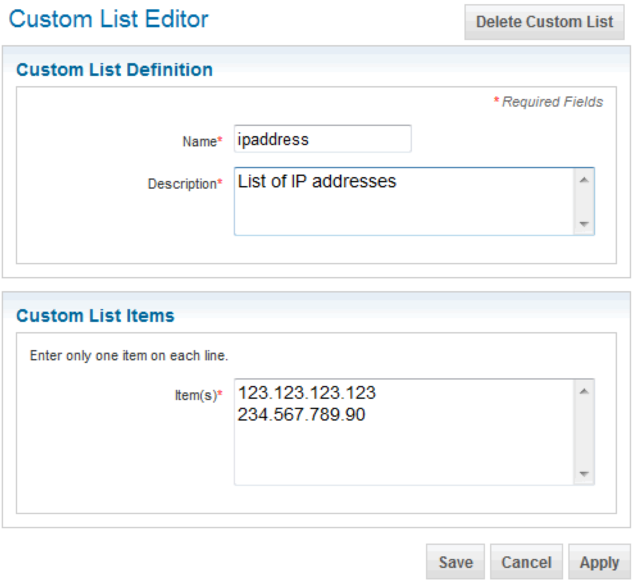
This example shows a rule for screening orders for suspicious attributes and activities of a specific proxy IP address. You need to create one condition for each comparison value that you choose.

Example 6 Rule That Screens for IP Address Characteristics

First set of conditions	
Order element	Proxy IP address activities
Comparison operator	contains
Comparison values	Phishing
	Nigerian email or spam
	UDP port scan
	TCP port scan
	Connecting to botnet
	Connecting to malware site
	Connecting to suspicious IRC server
	Click fraud
	Malware
	Spam
Second set of conditions	
Order element	Proxy IP address attributes
Comparison operator	contains
Comparison values	Bogon
	Hijacked
	Open relay
	Zombie or botnet
Condition relationship	At least one condition is true.
Profile setting	Review or reject orders that contain a true condition.

Custom Fields and Lists

Custom fields and lists enable you to customize rules with any operator in the condition editor. For example, you can create a list of IP addresses, as in the figure below. You can modify the items in the list as often as necessary. After you add the list to a custom rule, you can set the profile that contains the rule to review or reject orders depending on the IP addresses found in the orders.



Custom List Editor

Custom List Definition

* Required Fields

Name* ipaddress

Description* List of IP addresses

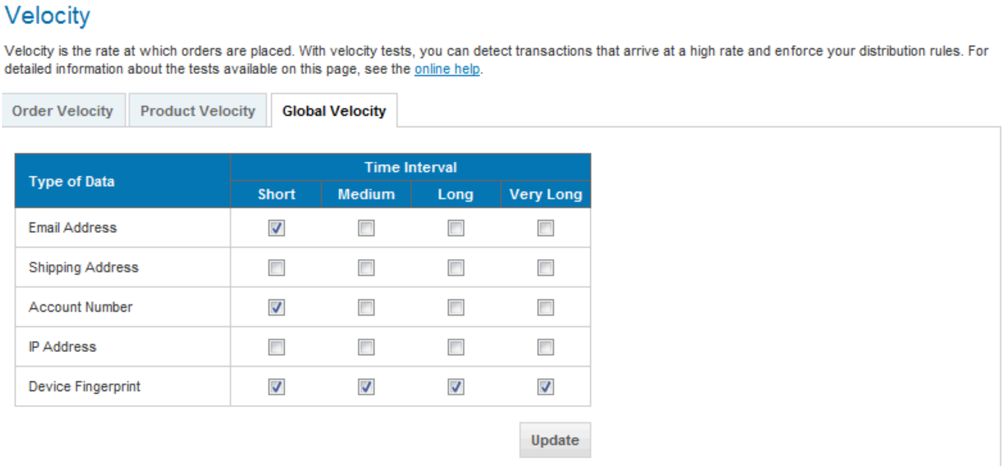
Custom List Items

Enter only one item on each line.

Item(s)* 123.123.123.123
234.567.789.90

Global Velocity

You can track device fingerprints at specific intervals in the Business Center. An information code is returned for each test that is triggered. By default, all time intervals are checked. False-positive results might occur during high-volume shopping periods. For example, during end-of-year holidays customers might make frequent purchases within a short period of time. During this time they might ship their gift purchases to different addresses, which might trigger other rules and also produce false-positive results. For more information, see the *Decision Manager Developer Guide Using the Simple Order API* (PDF | HTML), the *Decision Manager Developer Guide Using the SCMP API* (PDF | HTML), and the *Decision Manager User Guide* (PDF | HTML).



Velocity

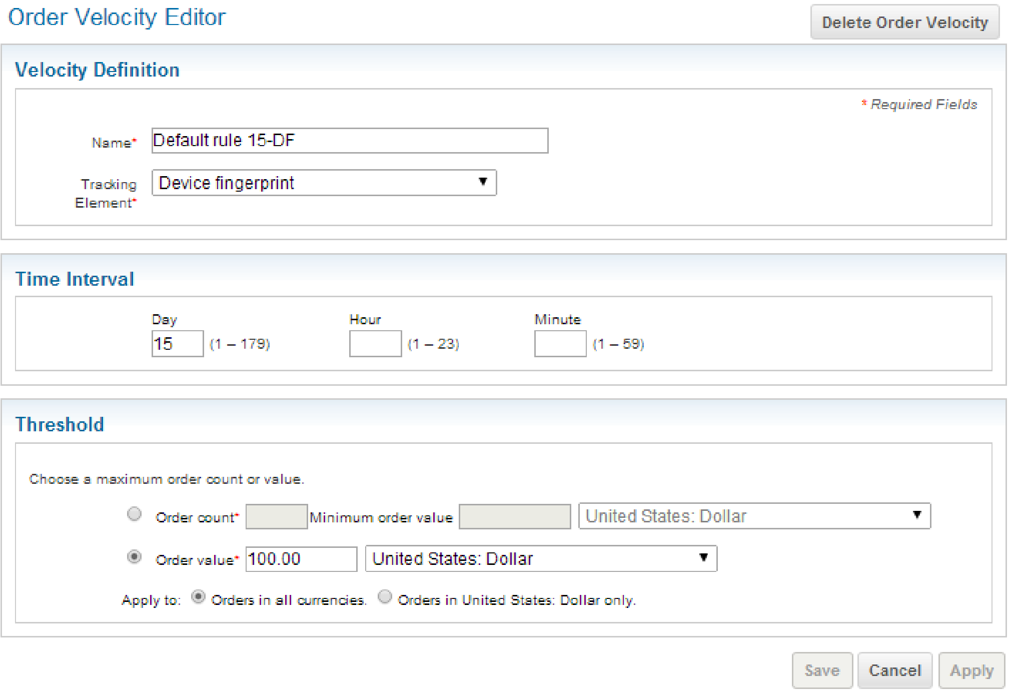
Velocity is the rate at which orders are placed. With velocity tests, you can detect transactions that arrive at a high rate and enforce your distribution rules. For detailed information about the tests available on this page, see the online help.

Type of Data	Time Interval			
	Short	Medium	Long	Very Long
Email Address	☑	☐	☐	☐
Shipping Address	☐	☐	☐	☐
Account Number	☑	☐	☐	☐
IP Address	☐	☐	☐	☐
Device Fingerprint	☑	☑	☑	☑

Order and Product Velocity

To evaluate the presence of a fingerprint in relation to product, time, number, or value of orders, you can create order and product velocity rules specific to your business needs.

This figure shows an order velocity rule that screens orders with a subtotal exceeding 100 USD for the presence of fingerprints. If a fingerprint occurs more than once every 14 days, the merchant receives an information code (MVEL-X).



Order Velocity Editor

Velocity Definition

* Required Fields

Name* Default rule 15-DF

Tracking Element* Device fingerprint

Time Interval

Day 15 (1 – 179) Hour (1 – 23) Minute (1 – 59)

Threshold

Choose a maximum order count or value.

○ Order count* Minimum order value United States: Dollar

● Order value* 100.00 United States: Dollar

Apply to: ● Orders in all currencies. ○ Orders in United States: Dollar only.

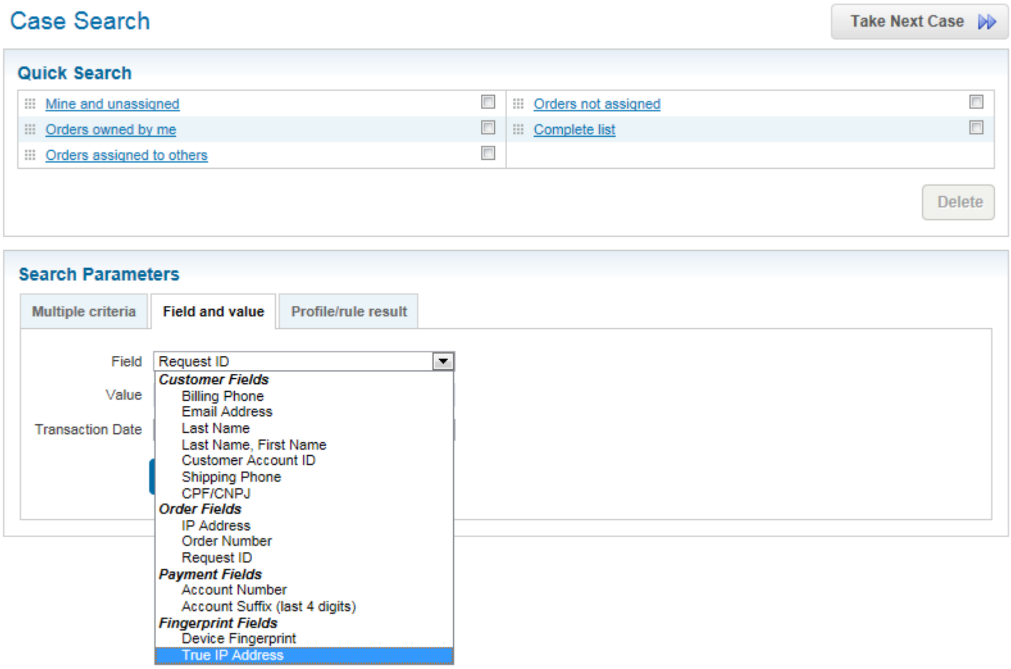
CHAPTER 3

Reviewing Orders

This chapter describes where you can view the encoded fingerprint in the Case Management and the Transaction Search nodes of the Business Center and how to use it to review orders. The encoded fingerprint appears as a string ending with an equal sign (=). For example: `77a8cbfbf3d7480e8aea4869eb1ca0c0=`. The fingerprint is stored in the fraud database with the rest of the transaction data for the same length of time (180 days).

Case Search

To search for device fingerprints, go to the Field and value tab in the Case Search window. When searching for a device fingerprint, you can specify any date range, but you cannot export the search results.

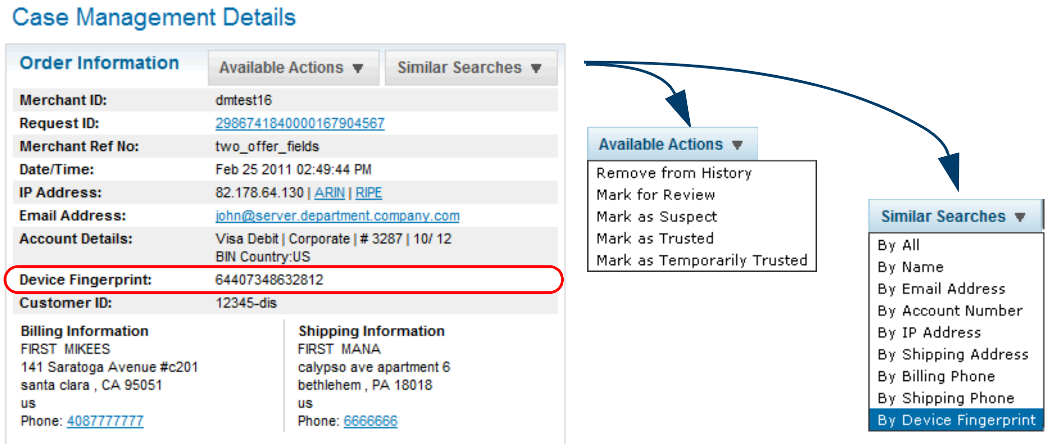


Field: Request ID

Case Management Details

If the fingerprint is available, more information might be available about the customer's identity and the device used to place the order. This figure shows the three areas of the Case Management Details window that you can use in your review process:

- Device Fingerprint link, which launches a dialog box with details about the device
- Available Actions menu, which you can use to mark the transaction
- Similar Searches menu, which you can use to search on the device fingerprint


Case Management Details

Order Information

Merchant ID:	dmtest16
Request ID:	2986741840000167904567
Merchant Ref No:	two_offer_fields
Date/Time:	Feb 25 2011 02:49:44 PM
IP Address:	82.178.64.130 | ARIN | RIPE
Email Address:	john@server.department.company.com
Account Details:	Visa Debit | Corporate | # 3287 | 10/ 12 BIN Country:US
Device Fingerprint:	64407348632812
Customer ID:	12345-dis

Billing Information
FIRST MIKEES
141 Saratoga Avenue #c201
santa clara , CA 95051
us
Phone: 4087777777

Shipping Information
FIRST MANA
calypso ave apartment 6
bethlehem , PA 18018
us
Phone: 6666666

Device Fingerprint Details

When you click the Device Fingerprint link in the Case Management Details window, the Device Fingerprint dialog appears, which contains information about the device. Sometimes, the link is present when the Smart ID is available instead of the fingerprint. Any of the fields below can contain information:

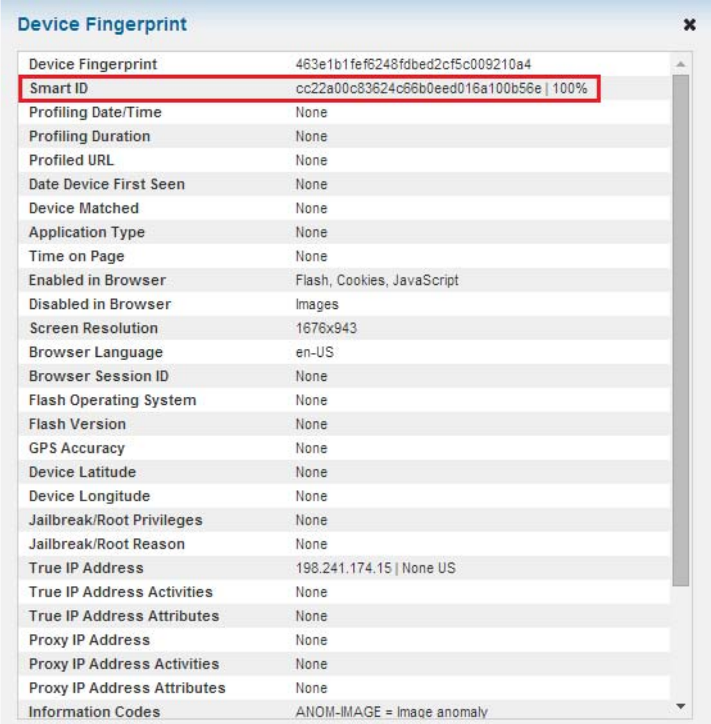
Table 2 Device Fingerprint Dialog Box Descriptions

Field	Description
Device Fingerprint	Unique ID of a computer or other device.
Smart ID	Device identifier generated from attributes collected during profiling. The confidence level follows the smart ID. Its value ranges from 0 to 100 and indicates the probability that the Smart ID is correctly identifying a returning device. A high percentage is more likely to represent a returning device than a new device that is similar to a previously identified device. As the confidence level decreases, the likelihood of a false positive increases.
Profiling Date/Time	Time of device profiling.
Profiling Duration	Total time in milliseconds to process the profiling request.
Profiled URL	URL of the profiled page.
Date Device First Seen	Date, in UTC, on which the device was first encountered.
Device Matched	Indicates whether the device was previously encountered and whether enough attributes were gathered to identify the device: ▪ `Success`: Device fingerprint was previously encountered. ▪ `New_Device`: Device was not previously encountered. ▪ `Not_Enough_Attribs`: Not enough attributes were gathered to indicate whether the device was previously encountered.
Application Type	Indicates whether the session was initiated from a mobile device or a computer. If the session is initiated from a mobile device, this field indicates whether the mobile browser or mobile application is being used: ▪ `browser_computer`: Device is using a standard browser, which contains the fingerprinting tags. ▪ `browser_mobile`: Device is using a mobile browser, which contains the fingerprinting tags. ▪ `agent_mobile`: Device is using a mobile application, and fingerprinting mobile SDK tags are present in that mobile application.
Time on Page	Time period in milliseconds that the device profiling page appears in the browser before it closes or the user navigates away from the page.
Enabled in Browser	Indicates whether Flash, images, JavaScript, or cookies are enabled in the device.

Table 2 Device Fingerprint Dialog Box Descriptions (Continued)

Field	Description
Disabled in Browser	Indicates whether Flash, images, JavaScript, or cookies are disabled in the device.
Screen Resolution	Screen resolution of the device, which can distinguish a computer from a mobile device.
Browser Language	Language detected in the browser, such as English or Japanese.
Browser Session ID	The concatenated merchant ID and session ID value that is sent in with the request. See deviceFingerprintID, page 43, if you are using the Simple Order API, or device_fingerprint_id, page 52, if you are using the SCMP API.
Flash Operating System	Device operating system as reported by Flash.
Flash Version	The version of Flash installed on the device.
GPS Accuracy	Indicates the accuracy of the GPS location of the device rounded up to the nearest meter measurement. For example, if the accuracy is determined to be within 17.9 meters, `18` is returned in the reply. Returned only for mobile devices.
Device Latitude	Latitude of the GPS location of the device returned in the format degrees.minutes. For example: `-37.82465426` Returned only for mobile devices.
Device Longitude	Longitude of the GPS location of the device returned in the format degrees.minutes. For example: `145.22554548` Returned only for mobile devices.
Jailbreak/Root Privileges	Indicates that a mobile device has root privileges. This form of privilege escalation is known as “jailbreaking” on iOS devices. This field returns a numerical value that indicates the number of root elements or “jailbreaks” are detected on the device. `0` indicates that there are no root elements or jailbreaks detected. Returned only for mobile devices.
Jailbreak/Root Reason	Additional information that describes the elements on the device that triggered the escalation to root privileges or “jailbreak.” See the field description for Jailbreak/Root Privileges. Returned only for mobile devices.
True IP Address	Customer’s IP address detected by the application.
True IP Address Activities	Actions associated with the true IP address.
True IP Address Attributes	Attributes associated with the true IP address.
Proxy IP Address	If applicable, IP address substituted for the true IP address.
Proxy IP Address Activities	Actions associated with the proxy IP address.
Proxy IP Address Attributes	Attributes associated with the proxy IP address.
Information Codes	Codes specific to the elements of the fingerprint.

The following figure shows the window that appears when you click the fingerprint link:



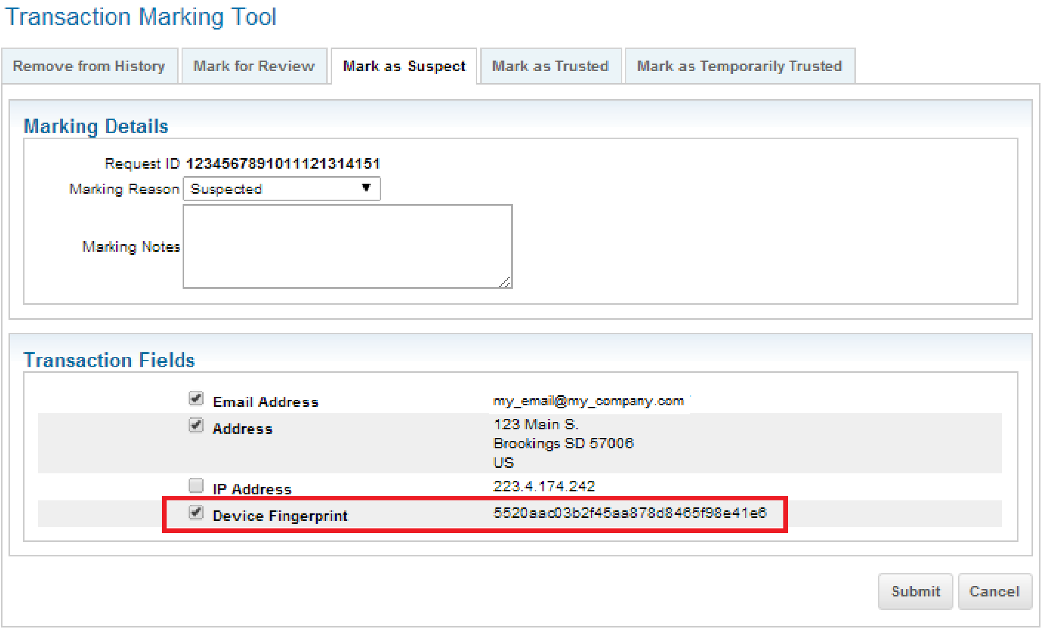
Device Fingerprint	463e1b1fef6248fdbed2cf5c009210a4
Smart ID	cc22a00c83624c66b0eed016a100b56e | 100%
Profiling Date/Time	None
Profiling Duration	None
Profiled URL	None
Date Device First Seen	None
Device Matched	None
Application Type	None
Time on Page	None
Enabled in Browser	Flash, Cookies, JavaScript
Disabled in Browser	Images
Screen Resolution	1676x943
Browser Language	en-US
Browser Session ID	None
Flash Operating System	None
Flash Version	None
GPS Accuracy	None
Device Latitude	None
Device Longitude	None
Jailbreak/Root Privileges	None
Jailbreak/Root Reason	None
True IP Address	198.241.174.15 | None US
True IP Address Activities	None
True IP Address Attributes	None
Proxy IP Address	None
Proxy IP Address Activities	None
Proxy IP Address Attributes	None
Information Codes	ANOM-IMAGE = Image anomaly

In the above example, you can view all the browser attributes and IP addresses:

- Cookies, Flash, and JavaScript are enabled, but images are disabled.
- The Smart ID is present with a confidence level of 100%, which suggests that the device was previously encountered.
- The high resolution detected implies a computer instead of a mobile device.
- The browser is set to U.S. English (`en-US`).
- The Information Code indicates that an image anomaly is detected.

Available Actions

Using the Available Actions menu in the Case Management Details window, you can add the fingerprint to your positive or negative list, or remove it from history. If you choose Mark as Suspect, the Transaction Marking Tool appears with all the data that you can add to the negative list for that order, including the fingerprint. The available data can differ from order to order. To add the fingerprint to your negative list, check the box in the Transaction Fields pane.



Request ID 12345678910111213141 51

Marking Reason: Suspected ▼

Marking Notes

☑ Email Address	my_email@my_company.com
☑ Address	123 Main S. Brookings SD 57006 US
☐ IP Address	223.4.174.242
☑ Device Fingerprint	5520aac03b2f45aa878d8465f98e41e6

Similar Searches

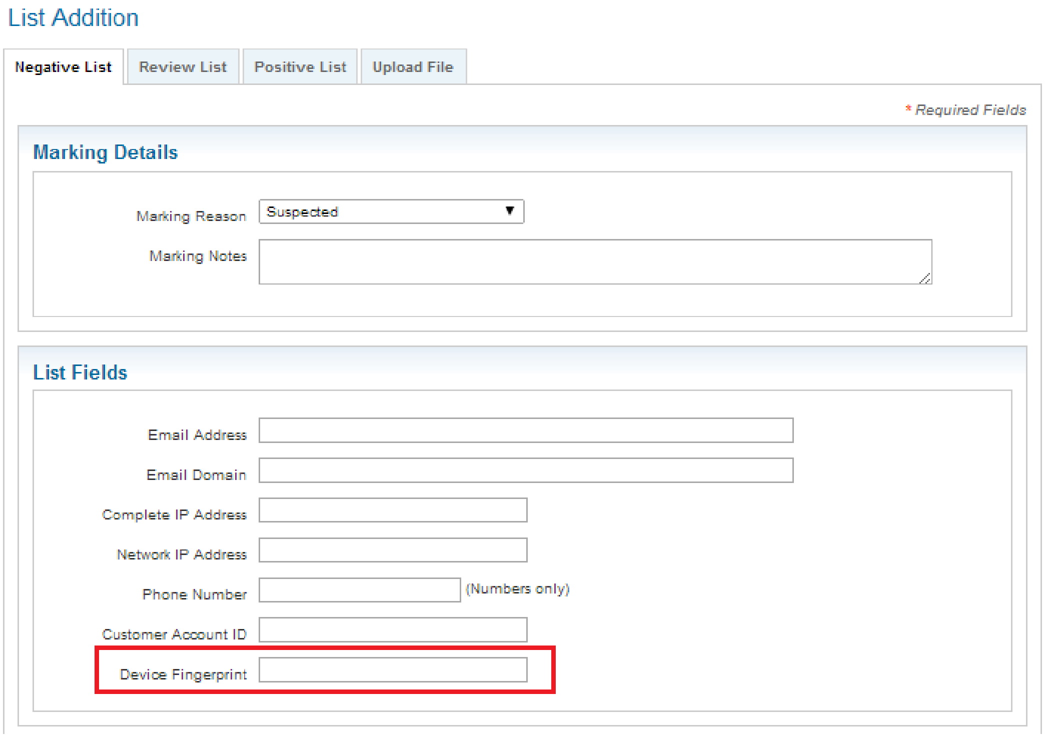
Using the Similar Searches menu in the Case Management Details window, you can review other orders placed from the same computer or device by searching for orders that contain the same device fingerprint. The menu options appear only when the data is present in the order. For example, you can search for other devices with the same fingerprint only when the current order contains a fingerprint. The Smart ID can also be used to search when a Smart ID is present in the order, and the confidence level is above a certain threshold.

The results table that is returned can contain up to 2,000 orders that correspond to your search parameters. To verify that you have the orders that you want, examine your search parameters, which are listed above the table. For example:

```
Results: Date: Aug 01 2013 12:00:00 AM - Feb 01 2014 06:55:49 PM |
Device Fingerprint 284928483475 | Transactions: 1568
```

Customer Lists

You can manually add device fingerprints to your positive or negative list from the List Addition window. (**Decision Manager > List Manager > List Addition**)

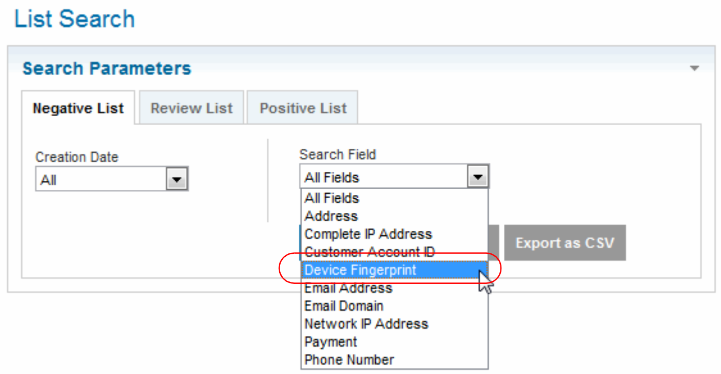


List Addition

Marking Reason: Suspected

Marking Notes:

You can also search customer lists for fingerprints. The fingerprint appears in downloaded reports.



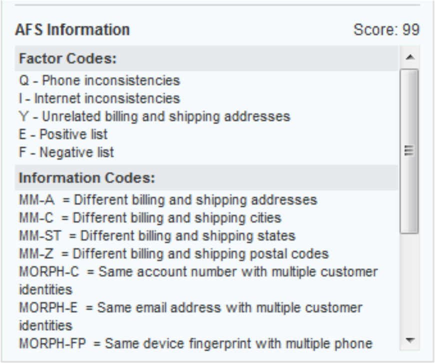
List Search

Creation Date: All

Search Field: All Fields

Information Codes

You can view information codes in the AFS Information pane of the Case Management Details window. In the following figure, the order is risky because the score is high (99), and the returned factor codes and information codes indicate inconsistencies in the order data.



AFS Information Score: 99

Factor Codes:

Q - Phone inconsistencies
I - Internet inconsistencies
Y - Unrelated billing and shipping addresses
E - Positive list
F - Negative list

Information Codes:

MM-A = Different billing and shipping addresses
MM-C = Different billing and shipping cities
MM-ST = Different billing and shipping states
MM-Z = Different billing and shipping postal codes
MORPH-C = Same account number with multiple customer identities
MORPH-E = Same email address with multiple customer identities
MORPH-FP = Same device fingerprint with multiple phone

APPENDIX A

API Fields and Information Codes

In addition to replacing the merchant and session IDs in your web page or your mobile application, you must send the session ID to CyberSource in your API request and be prepared to receive specific fields and information codes in the reply.

Simple Order API

Important

If you process call center orders, do not submit device fingerprint or IP address information in the request of those orders.

Request Fields

Table 3 Simple Order API Request Fields

Field	Description	Used By: Required (R) or Optional (O)	Data Type & Length
deviceFingerprintHash	Field that contains the unique identifier of the device that is returned in the afsReply_deviceFingerprint_hash API reply field. To use this request field, you must use version 1.103 or higher of the Simple Order API schema.	riskUpdate Service (O)	String (255)

Table 3 **Simple Order API Request Fields (Continued)**

Field	Description	Used By: Required (R) or Optional (O)	Data Type & Length
deviceFingerprintID	Field that contains the session ID that you send to Decision Manager to obtain the device fingerprint information. The string can contain uppercase and lowercase letters, digits, hyphen (-), and underscore (_). However, do not use the same uppercase and lowercase letters to indicate different session IDs. The session ID must be unique for each transaction and for each merchant ID. You can use any string that you are already generating, such as an order number or web session ID. To use this request field, you must use version 1.29 or later of the Simple Order API schema.	Decision Manager (O)	String (88)

Reply Fields

All of these reply fields are returned by the Advanced Fraud Screen service (**afsService**). To receive these reply fields, you must use version 1.49 or later of the Simple Order API schema unless it is noted otherwise in the field description.

Table 4 **Simple Order API Reply Fields**

Field	Description	Data Type & Length
afsReply_deviceFingerprint_agentType	Indicates whether a mobile device or a computer was used to initiate the session. If the session is initiated with a mobile device, this field indicates whether the mobile browser or mobile application is being used. This field can return the following values: ▪ `browser_computer`: Device is using a standard browser, which contains the fingerprinting tags. ▪ `browser_mobile`: Device is using a mobile browser, which contains the fingerprinting tags. ▪ `agent_mobile`: Device is using a mobile application, and fingerprinting mobile SDK tags are present in that mobile application. To receive this reply field, you must use version 1.100 or later of the Simple Order API schema.	String (255)

Table 4 Simple Order API Reply Fields (Continued)

Field	Description	Data Type & Length
afsReply_deviceFingerprint_ browserLanguage	Comma-separated list of languages preferred or supported by the browser. When the browser supports more than one language, a Q value between 0 and 1 can be assigned to each language to indicate which language the browser prefers or supports. The preferred language is assigned the default value of 1, which may be omitted from the string. Examples: ▪ `en-us, en;q=0`: the browser prefers U.S. English but can support non-U.S. English. ▪ `es, en-us; q=0.3, de;q=0.1`: the browser prefers Spanish (`es`) but can support U.S. English (`en-us;q=0.3`) and German (`de;q=0.1`).	String (255)
afsReply_deviceFingerprint_ cookiesEnabled	Indicates whether cookies are enabled in the customer's browser. This field can contain one of these values: ▪ `true` ▪ `false`	String (255)
afsReply_deviceFingerprint_ dateTime	The arrival time of the first fingerprint attribute for this session, expressed in the following format: YYYY-MM-DDThh:mm:ssZ For example: `2014-08-11T22:47:57Z` is equal to August 11, 2014, at 10:47:57 P.M. The T separates the date and the time. The Z indicates UTC. To receive this reply field, you must use version 1.100 or later of the Simple Order API schema.	String (255)
afsReply_deviceFingerprint_ deviceLatitude	Returned for mobile devices only. Latitude of the GPS location of the device returned in the format degrees.minutes. For example: `-37.82465426` To receive this reply field, you must use version 1.100 or later of the Simple Order API schema.	String (255)
afsReply_deviceFingerprint_ deviceLongitude	Returned for mobile devices only. Longitude of the GPS location of the device returned in the format degrees.minutes. For example: `145.22554548` To receive this reply field, you must use version 1.100 or later of the Simple Order API schema.	String (255)

Table 4 Simple Order API Reply Fields (Continued)

Field	Description	Data Type & Length
afsReply_deviceFingerprint_ deviceMatch	Indicates whether the device was encountered before and whether enough attributes were gathered to identify the device. This field can return the following values: ▪ `Success`: Device fingerprint was previously encountered. ▪ `New_Device`: Device was not previously encountered. ▪ `Not_Enough_Attribs`: Not enough attributes were gathered to identify whether the device was previously encountered. To receive this reply field, you must use version 1.100 or later of the Simple Order API schema.	String (255)
afsReply_deviceFingerprint_ firstEncounter	Date that the device was first encountered. This value is returned in the format: yyyy-mm-dd To receive this reply field, you must use version 1.100 or later of the Simple Order API schema.	String (255)
afsReply_deviceFingerprint_ flashEnabled	Whether Flash is enabled in the customer's browser. This field can contain one of these values: ▪ `true` ▪ `false`	String (255)
afsReply_deviceFingerprint_ flashOS	Device operating system as reported by Flash. To receive this reply field, you must use version 1.100 or later of the Simple Order API schema.	String (255)
afsReply_deviceFingerprint_ flashVersion	The version of Flash installed on the device. To receive this reply field, you must use version 1.100 or later of the Simple Order API schema.	String (255)
afsReply_deviceFingerprint_ gpsAccuracy	Returned for mobile devices only. Indicates the accuracy of the GPS location of the device rounded up to the nearest meter measurement. For example, if the accuracy is determined to be within 17.9 meters, `18` is returned in the reply. To receive this reply field, you must use version 1.100 or later of the Simple Order API schema.	String (255)
afsReply_deviceFingerprint_hash	Unique identifier of the computer.	String (255)
afsReply_deviceFingerprint_ imagesEnabled	Indicates whether images are enabled in the customer's browser. This field can contain one of these values: ▪ `true` ▪ `false`	String (255)

Table 4 Simple Order API Reply Fields (Continued)

Field	Description	Data Type & Length
afsReply_deviceFingerprint_javascriptEnabled	Indicates whether JavaScript is enabled in the customer's browser. This field can contain one of these values: ▪ `true` ▪ `false`	String (255)
afsReply_deviceFingerprint_jbRoot	Returned for mobile devices only. Detects whether a mobile device that is running the Decision Manager device fingerprinting mobile SDK has root privileges. This form of privilege escalation is known as "jailbreaking" on iOS devices. This field returns a numerical value that indicates the number of root elements or "jailbreaks" detected on the device. 0 indicates that there are no root elements or jailbreaks detected. To receive this reply field, you must use version 1.100 or later of the Simple Order API schema.	Integer (255)
afsReply_deviceFingerprint_jbRootReason	Returned for mobile devices only. Returns additional information that describes the elements on the device that triggered the escalation to root privileges. To receive this reply field, you must use version 1.100 or later of the Simple Order API schema.	String (255)
afsReply_deviceFingerprint_profileDuration	Total time in milliseconds to process the profiling request. To receive this reply field, you must use version 1.100 or later of the Simple Order API schema.	Integer (255)
afsReply_deviceFingerprint_profiledURL	URL of the profiled page. If the device fingerprinting mobile SDK is used, this reply field returns the Custom URL that was specified in the `doProfileRequest()` function of your mobile application. See Step 3 of "Implementing the Device Fingerprinting SDK in Android Applications," page 18, or Step 4 of "Implementing the Device Fingerprinting SDK in iOS Applications," page 20. To receive this reply field, you must use version 1.100 or later of the Simple Order API schema.	String (255)
afsReply_deviceFingerprint_proxyIPAddress	IP address of the proxy if it is available.	String (255)

Table 4 Simple Order API Reply Fields (Continued)

Field	Description	Data Type & Length
afsReply_deviceFingerprint_ proxyIPAddressActivities	Actions associated with the proxy IP address. This field can contain one or more of these values, separated by carets (^): ■ `BANK`: IP address belongs to a financial organization. ■ `CLICK_FRAUD`: IP address has been used for click fraud. ■ `CONNECTING_TO_BOTNET`: IP address has been connected to a botnet. ■ `CONNECTING_TO_MALWARE_SITE`: IP address has been connected to a malware site. ■ `DNS_CONNECTION_ANOMALY`: IP address has had DNS connection anomaly. ■ `INSTANT_MSG`: IP address has been used for instant messaging. ■ `IRC_CONNECTION_ANOMALY`: IP address has been connected to a suspicious IRC server. ■ `LEGITIMATE`: IP address has been legitimate. ■ `MALWARE`: IP address has been used for malware. ■ `NIGERIAN`: IP address has been used for Nigerian email or spam. ■ `OTHER`: IP has been involved in other activities. ■ `P2P`: IP address has been used for peer-to-peer communication. ■ `PHISH`: IP address has been used for phishing. ■ `SPAM`: IP address has been used to send spam. ■ `TCP_SCAN_FLAG`: IP address has been used as TCP port scanner. ■ `UDP_SCAN_FLAG`: IP address has been used as UDP port scanner.	String (255)

Table 4 Simple Order API Reply Fields (Continued)

Field	Description	Data Type & Length
afsReply_deviceFingerprint_ proxyIPAddressAttributes	Characteristics associated with the proxy IP address. This field can contain one or more of these values, separated by carets (^): ▪ BOGON: IP address has been part of the bogon ranges. ▪ BOTNET_ZOMBIE: IP address has been either a zombie or a botnet. ▪ DYNAMIC: IP address has been dynamic. ▪ HIJACKED: IP address has been part of the hijacked ranges. ▪ NAME_SERVER: IP address has been a name server. ▪ OPEN_PROXY: IP address has been an open proxy. ▪ OPEN_RELAY: IP address has been an open relay. ▪ PORTAL: IP address has been a portal. ▪ PROXY: IP address has been a proxy. ▪ RANGE: IP address has been part of an IP range. ▪ STATIC: IP address has been static.	String (255)
afsReply_deviceFingerprint_ proxyServerType	Type of proxy server based on the HTTP header. This field can contain one of these values: ▪ Anonymous: presence of an HTTP header indicates the presence of a proxy but does not disclose the client IP address. ▪ Hidden: absence of an HTTP header indicates the presence of a proxy attempting to hide its purpose. Often returned for compromised servers or botnets that are used as proxies. ▪ Transparent: presence of an HTTP header indicates the presence of a proxy and discloses the client IP address. This value usually corresponds to a proxy that filters corporate or ISP content. This value is the safest.	String (255)
afsReply_deviceFingerprint_ screenResolution	Screen resolution of the device. The value is a number in the format nnnnXmmmm.	String (255)
afsReply_deviceFingerprint_ smartID	Device identifier generated from attributes collected during profiling.	String (255)
afsReply_deviceFingerprint_ smartIDConfidenceLevel	Probability that the Smart ID is correctly identifying a returning device. The value ranges from 0 to 100. A high number is more likely to represent a returning device than a new device similar to a previously identified device. As the confidence level decreases, the probability of false positives increases.	Integer (3)

Table 4 Simple Order API Reply Fields (Continued)

Field	Description	Data Type & Length
afsReply_deviceFingerprint_ timeOnPage	Time period in milliseconds that the device profiling page displays on the browser before it closes or the user navigates away from the page. To receive this reply field, you must use version 1.100 or later of the Simple Order API schema.	Integer (255)
afsReply_deviceFingerprint_ trueIPAddress	Customer's true IP address detected by the application.	String (255)
afsReply_deviceFingerprint_ trueIPAddressActivities	Actions associated with the true IP address. This field can contain one or more of these values, separated by carets (^): ■ `BANK`: IP address belongs to a financial organization. ■ `CLICK_FRAUD`: IP address has been used for click fraud. ■ `CONNECTING_TO_BOTNET`: IP address has been connected to a botnet. ■ `CONNECTING_TO_MALWARE_SITE`: IP address has been connected to a malware site. ■ `DNS_CONNECTION_ANOMALY`: IP address has had a DNS connection anomaly. ■ `INSTANT_MSG`: IP address has been used for instant messaging. ■ `IRC_CONNECTION_ANOMALY`: IP address has been connected to a suspicious IRC server. ■ `LEGITIMATE`: IP address has been legitimate. ■ `MALWARE`: IP address has been used for malware. ■ `NIGERIAN`: IP address has been used for Nigerian email or spam. ■ `OTHER`: IP has been involved in other activities. ■ `P2P`: IP address has been used for peer-to-peer communication. ■ `PHISH`: IP address has been used for phishing. ■ `SPAM`: IP address has been used to send spam. ■ `TCP_SCAN_FLAG`: IP address has been used as TCP port scanner. ■ `UDP_SCAN_FLAG`: IP address has been used as UDP port scanner.	String (255)

Table 4 Simple Order API Reply Fields (Continued)

Field	Description	Data Type & Length
afsReply_deviceFingerprint_trueIPAddressAttributes	Characteristics associated with the true IP address. This field can contain one or more information codes, separated by carets (^). This field can contain one of these values: ■ BOGON: IP address has been part of the bogon ranges. ■ BOTNET_ZOMBIE: IP address has been either a zombie or a botnet. ■ DYNAMIC: IP address has been dynamic. ■ HIJACKED: IP address has been part of the hijacked ranges. ■ NAME_SERVER: IP address has been a name server. ■ OPEN_PROXY: IP address has been an open proxy. ■ OPEN_RELAY: IP address has been an open relay. ■ PORTAL: IP address has been a portal. ■ PROXY: IP address has been a proxy. ■ RANGE: IP address has been part of an IP range. ■ STATIC: IP address has been static.	String (255)
afsReply_deviceFingerprint_trueIPCity	City associated with the true IP address. If the data is available, the content of this field is more reliable than other city information in the order because any cloaking by the customer has been removed.	String (255)
afsReply_deviceFingerprint_trueIPAddressCountry	Country associated with the true IP address. If the data is available, the content of this field is the more reliable than other country information in the order because any cloaking by the customer has been removed.	String (255)
afsReply_identityInfoCode	Change in customer identity elements. This field can contain one or more codes, separated by carets (^), for example: MORPH-C^MORPH-B. For a list of values, see "Excessive Customer Identity Changes," page 63.	String (255)
afsReply_suspiciousInfoCode	The customer provided potentially suspicious information. This field can contain one or more codes, separated by carets (^), for example: BAD-FP^MM-TZTLO. For a list of values, see "Suspicious Data Information Codes," page 61.	String (255)
afsReply_velocityInfoCode	Customer has a high order velocity. This field can contain one or more codes, separated by carets (^), for example: VELS-TIP^VELI-TIP. For a list of values, see "Global Velocity," page 61.	String (255)

Simple Order API Request and Reply Examples

These examples show only the minimum fields required to process the order.

Request

```
billTo_<address_fields>=Customer’s billing information
shipTo_<address_fields>=Customer’s shipping information
card_<account_information>=Customer’s account information
billTo_ipAddress=12.345.67.890
billTo_firstName=john
billTo_lastName=doe
billTo_email=jdoe@example.com
deviceFingerprintID=7685380BB8A476AB4C21FE705DC3AA66
afsService_run=true
purchaseTotals_currency=USD
item_0_unitPrice=1.00
```

Reply

```
afsReply_suspiciousInfoCode=BAD-FP^INTL-BIN^MM-TZTLO^MUL-EM^RISK-DEV
afsReply_afsFactorCode=F
afsReply_afsResult=99
afsReply_hostSeverity=1
afsReply_identityInfoCode=MORPH-B^MORPH-C^MORPH-FB^MORPH-FE^MORPH-FP
afsReply_internetInfoCode=MM-IPBC
afsReply_ipCity=los angeles
afsReply_ipCountry=us
afsReply_ipRoutingMethod=standard
afsReply_ipState=ca
afsReply_reasonCode=481
afsReply_velocityInfoCode=VELS-FP
afsReply_deviceFingerprint_cookiesEnabled=true
afsReply_deviceFingerprint_flashEnabled=true
afsReply_deviceFingerprint_imagesEnabled=false
afsReply_deviceFingerprint_javascriptEnabled=true
afsReply_deviceFingerprint_trueIPAddress=66.185.179.2
afsReply_deviceFingerprint_smartID=278682734918374
afsReply_deviceFingerprint_smartIDConfidenceLevel=96
decision=REJECT
merchantReferenceCode=10679256010963322294714
purchaseTotals_currency=USD
reasonCode=481
```

SCMP API

Important If you process call center orders, do not submit device fingerprint or IP address information in the request of those orders.

Request Fields

Table 5 SCMP API Request Field

Field	Description	Used By: Required (R) or Optional (O)	Data Type & Length
device_fingerprint_hash	Field that contains the unique identifier of the device that is returned in the score_device_fingerprint_hash API reply field.	ics_risk_update (O)	String (255)
device_fingerprint_id	Field that contains the session ID that you send to Decision Manager to obtain the device fingerprint information. The string can contain uppercase and lowercase letters, digits, hyphen (-), and underscore (_). However, do not use the same uppercase and lowercase letters to indicate different session IDs. The session ID must be unique for each merchant ID. You can use any string that you are already generating, such as an order number or web session ID.	Decision Manager (O)	String (88)

Reply Fields

These reply fields are all returned by the **ics_score** service.

Table 6 SCMP API Reply Fields

Field	Description	Data Type & Length
score_device_fingerprint_agent_type	Indicates whether a mobile device or a computer was used to initiate the session. If the session is initiated with a mobile device, this field indicates whether the mobile browser or mobile application is being used. This field can return the following values: ■ `browser_computer`: Device is using a standard browser, which contains the fingerprinting tags. ■ `browser_mobile`: Device is using a mobile browser, which contains the fingerprinting tags. ■ `agent_mobile`: Device is using a mobile application, and fingerprinting mobile SDK tags are present in that mobile application.	String (255)
score_device_fingerprint_browser_language	Comma-separated list of languages preferred or supported by the browser. When the browser supports more than one language, a Q value between 0 and 1 can be assigned to each language to indicate which language the browser prefers or supports. The preferred language is assigned the default value of 1, which may be omitted from the string. Examples: ■ `en-us, en;q=0`: the browser prefers U.S. English but can support non-U.S. English. ■ `es, en-us; q=0.3, de;q=0.1`: the browser prefers Spanish (`es`) but can support U.S. English (`en-us;q=0.3`) and German (`de;q=0.1`).	String (255)
score_device_fingerprint_cookies_enabled	Indicates whether cookies are enabled in the customer's browser. This field can contain one of these values: ■ `true` ■ `false`	String (255)
score_device_fingerprint_date_time	The arrival time of the first fingerprint attribute for this session, expressed in the following format: YYYY-MM-DDThhmmssZ For example: `2014-08-11T224757Z` is equal to August 11, 2014, at 10:47:57 P.M. The T separates the date and the time. The Z indicates UTC.	String (255)

Table 6 SCMP API Reply Fields (Continued)

Field	Description	Data Type & Length
score_device_fingerprint_device_ latitude	Returned for mobile devices only. Latitude of the GPS location of the device returned in the format degrees.minutes. For example: `-37.82465426`	Decimal (255)
score_device_fingerprint_device_ longitude	Returned for mobile devices only. Longitude of the GPS location of the device returned in the format degrees.minutes. For example: `145.22554548`	Decimal (255)
score_device_fingerprint_device_ match	Indicates whether the device was encountered before and whether enough attributes were gathered to identify the device. This field can return the following values: ■ `Success`: Device fingerprint was previously encountered. ■ `New_Device`: Device was not previously encountered. ■ `Not_Enough_Attribs`: Not enough attributes were gathered to identify whether the device was previously encountered.	String (255)
score_device_fingerprint_first_ encounter	Date that the device was first encountered. This value is returned in the format: yyyy-mm-dd	String (255)
score_device_fingerprint_flash_ enabled	Whether Flash is enabled in the customer's browser. This field can contain one of these values: ■ `true` ■ `false`	String (255)
score_device_fingerprint_flash_os	Device operating system as reported by Flash.	String (255)
score_device_fingerprint_flash_ version	The version of Flash installed on the device.	String (255)
score_device_fingerprint_gps_ accuracy	Returned for mobile devices only. Indicates the accuracy of the GPS location of the device rounded up to the nearest meter. For example, if the accuracy is determined to be within 17.9 meters, `18` is returned in the reply.	Decimal (255)
score_device_fingerprint_hash	Unique identifier of the computer.	String (255)
score_device_fingerprint_images_ enabled	Indicates whether images are enabled in the customer's browser. This field can contain one of these values: ■ `true` ■ `false`	String (255)

Table 6 SCMP API Reply Fields (Continued)

Field	Description	Data Type & Length
score_device_fingerprint_javascript_enabled	Whether JavaScript is enabled in the customer's browser. This field can contain one of these values: ▪ `true` ▪ `false`	String (255)
score_device_fingerprint_jb_root	Returned for mobile devices only. Detects whether a mobile device that is running the Decision Manager device fingerprinting mobile SDK has root privileges. This form of privilege escalation is known as "jailbreaking" on iOS devices. This field returns a numerical value that indicates the number of root elements or "jailbreaks" detected on the device. 0 indicates that there are no root elements or jailbreaks detected.	Integer (255)
score_device_fingerprint_jb_root_reason	Returned for mobile devices only. Returns additional information that describes the elements on the device that triggered the escalation to root privileges.	String (255)
score_device_fingerprint_profile_duration	Total time in milliseconds to process the profiling request.	Integer (255)
score_device_fingerprint_profiled_url	URL of the profiled page. If the device fingerprinting mobile SDK is used, this reply field returns the Custom URL that was specified in the `doProfileRequest()` function of your mobile application. See Step 3 of "Implementing the Device Fingerprinting SDK in Android Applications," page 18, or Step 4 of "Implementing the Device Fingerprinting SDK in iOS Applications," page 20.	String (255)
score_device_fingerprint_proxy_ipaddress	IP address of the proxy if it is available.	String (255)

Table 6 SCMP API Reply Fields (Continued)

Field	Description	Data Type & Length
score_device_fingerprint_proxy_ ipaddress_activities	Actions associated with the proxy IP address. This field can contain one or more of these values, separated by carets (^): ■ BANK: IP address belongs to a financial organization. ■ CLICK_FRAUD: IP address has been used for click fraud. ■ CONNECTING_TO_BOTNET: IP address has been connected to a botnet. ■ CONNECTING_TO_MALWARE_SITE: IP address has been connected to a malware site. ■ DNS_CONNECTION_ANOMALY: IP address has had a DNS connection anomaly. ■ INSTANT_MSG: IP address has been used for instant messaging. ■ IRC_CONNECTION_ANOMALY: IP address has been connected to a suspicious IRC server. ■ LEGITIMATE: IP address has been legitimate. ■ MALWARE: IP address has been used for malware. ■ NIGERIAN: IP address has been used for Nigerian email or spam. ■ OTHER: IP has been involved in other activities. ■ P2P: IP address has been used for peer-to-peer communication. ■ PHISH: IP address has been used for phishing. ■ SPAM: IP address has been used to send spam. ■ TCP_SCAN_FLAG: IP address has been used as TCP port scanner. ■ UDP_SCAN_FLAG: IP address has been used as UDP port scanner.	String (255)

Table 6 SCMP API Reply Fields (Continued)

Field	Description	Data Type & Length
score_device_fingerprint_proxy_ ipaddress_attributes	Characteristics of the proxy IP address. This field can contain one or more of these values, separated by carets (^): ■ BOGON: IP address has been part of the bogon ranges. ■ BOTNET_ZOMBIE: IP address has been either a zombie or a botnet. ■ DYNAMIC: IP address has been dynamic. ■ HIJACKED: IP address has been part of the hijacked ranges. ■ NAME_SERVER: IP address has been a name server. ■ OPEN_PROXY: IP address has been an open proxy. ■ OPEN_RELAY: IP address has been an open relay. ■ PORTAL: IP address has been a portal. ■ PROXY: IP address has been a proxy. ■ RANGE: IP address has been part of an IP range. ■ STATIC: IP address has been static.	String (255)
score_device_fingerprint_proxy_ server_type	Type of proxy server based on the HTTP header. This field can contain one of these values: ■ Anonymous: presence of an HTTP header indicates the presence of a proxy but does not disclose the client IP address. ■ Hidden: absence of an HTTP header indicates the presence of a proxy attempting to hide its purpose. Often returned for compromised servers or botnets that are used as proxies. ■ Transparent: presence of an HTTP header indicates the presence of a proxy and discloses the client IP address. This value usually corresponds to a proxy that filters corporate or ISP content. This value is the safest.	String (255)
score_device_fingerprint_screen_ resolution	Screen resolution of the device. The value is a number in the format nnnnXmmmm.	String (255)
score_device_fingerprint_smart_id	Device identifier generated from attributes collected during profiling.	String (255)
score_device_fingerprint_smart_id_ confidence_level	Probability that the Smart ID is correctly identifying a returning device. The value ranges from 0 to 100. A high number is more likely to represent a returning device than a new device similar to a previously identified device. As the confidence level decreases, the likelihood of false positives increases.	Integer (3)
score_device_fingerprint_time_on_ page	Time period in milliseconds that the device profiling page displays on the browser before it closes or the user navigates away from the page.	Integer (255)

Table 6 SCMP API Reply Fields (Continued)

Field	Description	Data Type & Length
score_device_fingerprint_true_ ipaddress	True customer's IP address detected by the application.	String (255)
score_device_fingerprint_true_ ipaddress_activities	Actions associated with the true IP Address. This field can contain one or more of these values, separated by carets (^): ▪ BANK: IP address belongs to a financial organization. ▪ CLICK_FRAUD: IP address has been used for click fraud. ▪ CONNECTING_TO_BOTNET: IP address has been connected to a botnet. ▪ CONNECTING_TO_MALWARE_SITE: IP address has been connected to a malware site. ▪ DNS_CONNECTION_ANOMALY: IP address has had DNS connection anomaly. ▪ INSTANT_MSG: IP address has been used for instant messaging. ▪ IRC_CONNECTION_ANOMALY: IP address has been connected to a suspicious IRC server. ▪ LEGITIMATE: IP address has been legitimate. ▪ MALWARE: IP address has been used for malware. ▪ NIGERIAN: IP address has been used for Nigerian email or spam. ▪ OTHER: IP has been involved in other activities. ▪ P2P: IP address has been used for peer-to-peer communication. ▪ PHISH: IP address has been used for phishing. ▪ SPAM: IP address has been used to send spam. ▪ TCP_SCAN_FLAG: IP address has been used as TCP port scanner. ▪ UDP_SCAN_FLAG: IP address has been used as UDP port scanner.	String (255)

Table 6 SCMP API Reply Fields (Continued)

Field	Description	Data Type & Length
score_device_fingerprint_true_ ipaddress_attributes	Characteristics of the true IP address. This field can contain one or more information codes, separated by carets (^). This field can contain one of these values: - BOGON: IP address has been part of the bogon ranges. - BOTNET_ZOMBIE: IP address has been either a zombie or a botnet. - DYNAMIC: IP address has been dynamic. - HIJACKED: IP address has been part of the hijacked ranges. - NAME_SERVER: IP address has been a name server. - OPEN_PROXY: IP address has been an open proxy. - OPEN_RELAY: IP address has been an open relay. - PORTAL: IP address has been a portal. - PROXY: IP address has been a proxy. - RANGE: IP address has been part of an IP range. - STATIC: IP address has been static.	String (255)
score_device_fingerprint_true_ ipaddress_city	City associated with the true IP address. If the data is available, the content of this field is more reliable than other city information in the order because any cloaking by the customer has been removed.	String (255)
score_device_fingerprint_true_ ipaddress_country	Country associated with the true IP address. If the data is available, the content of this field is more reliable than other country information in the order because any cloaking by the customer has been removed.	String (255)
score_identity_info	Change in customer identity elements, such as address or account number. This field can contain one or more codes, separated by carets (^), for example: MORPH-C^MORPH-B. For a list of values, see "Information Codes," page 61.	String (255)
score_suspicious_info	The customer provided potentially suspicious information. This field can contain one or more codes, separated by carets (^), for example: BAD-FP^MM-TZTLO. For a list of values, see "Suspicious Data Information Codes," page 61.	String (255)
score_velocity_info	Customer has a high order velocity. This field can contain one or more codes, separated by carets (^), for example: VELS-TIP^VELI-TIP. For a list of values, see "Global Velocity," page 61.	String (255)

SCMP API Request and Reply Examples

These examples show only the minimum fields required to process the order.

Request

```
bill_<address_fields>=Customer’s billing address
ship_to_<address_fields>=Customer’s shipping address
customer_<account_information>=Customer’s account information
customer_ipaddress=12.345.67.890
customer_firstname=john
customer_lastname=doe
customer_email=jdoe@example.com
device_fingerprint_id=7685380BB8A476AB4C21FE705DC3AA66
ics_applications=ics_score
currency=USD
merchant_ref_number=10679256010963322294714
offer0=amount:1.00
```

Reply

```
score_address_info=COR-BA^MM-A^MM-C^MM-ST^MM-Z^UNV-ADDR
score_suspicious_info=BAD-FP^INTL-BIN^MM-TZTLO^MUL-EM^NON-LN^RISK-DEV
score_factors=Y
score_host_severity=1
score_identity_info=MORPH-B^MORPH-C^MORPH-FB^MORPH-FE^MORPH-FP
score_internet_info=MM-IPBC
score_ip_city=los angeles
score_ip_country=us
score_ip_routing_method=standard
score_ip_state=ca
score_device_fingerprint_cookies_enabled=true
score_device_fingerprint_flash_enabled=true
score_device_fingerprint_images_enabled=false
score_device_fingerprint_javascript_enabled=true
score_device_fingerprint_true_ipaddress=66.185.179.2
score_device_fingerprint_smart_id=278682734918374
score_device_fingerprint_smart_id_confidence_level=96
score_rcode=0
score_rflag=REJECT
score_rmsg=...reject...
score_score_result=99
score_velocity_info=VELS-FP
```

Information Codes

Global Velocity

Codes	Description
VELS-TIP	The true IP address has been used several times during the short interval.
VELI-TIP	The true IP address has been used several times during the medium interval.
VELL-TIP	The true IP address has been used several times during the long interval.

Suspicious Data Information Codes

Codes	Description
ANOM-BLANG	The browser string contains unusual words or patterns.
ANOM-BSTR	The browser string contains unexpected information.
ANOM-FLASH	Flash is installed but not enabled.
ANOM-IMAGE	An anomaly was detected that is associated with images loading in the browser.
ANOM-LANG	An anomaly was detected that is associated with the browser’s language setting.
ANOM-OS	The operating system indicated by the browser is inconsistent with the operating system that is detected with other system checks.
ANOM-SESS	An unexpected change occurred in the session.
ANOM-SRAT	The screen aspect ratio is outside the expected ranges.
ANOM-SRES	The screen resolution is outside the expected ranges.
ANOM-TZO	The time zone offset is inconsistent with the operating system.
BAD-FP	The device is risky.
DEV-MOB	The Smart ID detected a mobile device.
MASK-FP	The device history is masked.
MM-TZTLO	The device's time zone is inconsistent with the country's time zones.
NEW-FP	The Smart ID detected a new device.
RISK-DEV	Some of the device characteristics are risky.
RISK-PIP	The proxy IP address is risky. It was recently used as botnet or for spam or hacking purposes.
RISK-TIP	The true IP address is risky. It was recently used as botnet or for spam or hacking purposes.

Excessive Digital Identity Changes

Codes	Description
MORPH-FB	The device fingerprint has occurred several times with multiple billing addresses.
MORPH-FC	The device fingerprint has occurred several times with multiple account numbers.
MORPH-FE	The device fingerprint has occurred several times with multiple email addresses.
MORPH-FI	The device fingerprint has occurred several times with multiple IP addresses.
MORPH-FP	The device fingerprint has occurred several times with multiple phone numbers.
MORPH-FPIP	The device fingerprint has occurred several times with multiple proxy IP addresses.
MORPH-FPLO	The device fingerprint has occurred several times in multiple proxy IP address locations.
MORPH-FRES	The device fingerprint has occurred several times with multiple screen resolutions.
MORPH-FS	The device fingerprint has occurred several times with multiple shipping addresses.
MORPH-FTIP	The device fingerprint has occurred several times with multiple true IP addresses.
MORPH-FTLO	The device fingerprint has been used several times in multiple true IP address locations.
MORPH-FTZ	The device fingerprint has occurred several times in multiple time zones.
MORPH-TF	The true IP address has occurred several times with multiple devices.
MORPH-TPIP	The true IP address has occurred several times with multiple proxy IP addresses.
MORPH-TPLO	The true IP address has occurred several times in multiple proxy IP address locations.
MORPH-TRES	The true IP address has occurred several times with multiple screen resolutions.
MORPH-TTZ	The true IP address has occurred several times in multiple time zones.

Excessive Customer Identity Changes

You receive an information code when more than two identity changes occur for one customer. *Customer identity* refers to one or more of these elements: account and phone numbers, billing, shipping, fingerprint, email, and IP addresses.

Codes	Description
MORPH-B	The billing address has been used several times with multiple customer identities.
MORPH-C	The account number has been used several times with multiple customer identities.
MORPH-E	The email address has been used several times with multiple customer identities.
MORPH-I	The IP address has been used several times with multiple customer identities.
MORPH-P	The phone number has been used several times with multiple customer identities.
MORPH-S	The shipping address has been used several times with multiple customer identities.

APPENDIX

B

Device Fingerprinting Cookie FAQ

Because of developing regulations regarding cookie usage in the European Union,[1] CyberSource has received questions about how its services use cookies. This information is included here because CyberSource Decision Manager Device Fingerprinting uses cookies.

1 What is a cookie?

A cookie is a small file, typically consisting of letters and numbers, which is downloaded to and stored on a user's computer or other electronic device when the user visits certain web sites. Information from cookies is used for a variety of purposes. For example, cookies can be used to enhance security or configure a web site to make it more convenient for a visitor.

2 Does CyberSource Decision Manager set cookies on users' computers?

Yes, but only if you are using device fingerprinting as part of Decision Manager. If you are not using device fingerprinting, Decision Manager does not set any cookies.

3 What purpose does the cookie serve? Will the service function without the cookie?[1]

If you are using device fingerprinting, Decision Manager drops one cookie as described in the following chart:

Purpose	**Data Stored**	**Will the service function without the cookie?**	**Persistent?**
Provides identification of a returning device.	The user's device fingerprint, generated by CyberSource's device fingerprint technology vendor.	Yes.	Yes, for five years.

[1] This information is not intended to be legal advice. CyberSource recommends that you seek advice from independent counsel regarding your obligations regarding the use of cookies under applicable law.

4 Does CyberSource obtain user consent for this cookie?

No. CyberSource is a third-party vendor and does not have contact or a direct relationship with your users. Under your agreement with CyberSource, it is the merchant’s responsibility to provide their users any legally required notices or obtain necessary consent in order to set cookies.

Please contact us if you have any questions.