

ACI RED SHIELD® CSI-2 TIEBACK GUIDE

VERSION 1.5

SHAUN HUGHES
JUNE 2017



Table of contents

1. Introduction	3
1.1 ACI ReD Shield ®	3
1.2 ACI ReD Shield ® Customer Service Interface	3
1.3 Case Manager.....	3
2. Tieback.....	4
2.1 Tieback High Level Process Flow.....	4
3. Implementing Tieback	5
3.1 HTTP Messaging	5
4. Creating the Tieback Message Request.....	6
4.1 Tieback Keys.....	6
4.2 Sample Tieback Message Request	6
4.3 Sample Message Content.....	7
4.3.1 Approve	7
4.3.2 Cancel	7
4.3.3 Pend	7
5. Response.....	8
6. Client Testing	8
7. Failed Tiebacks	10
8. Cipher List	11
9. Revision History.....	13

1. Introduction

1.1 ACI ReD Shield ®

ACI ReD Shield® is a real-time fraud prevention solution tailored to the needs of eCommerce merchants and payment service providers (PSPs). The solution is designed to enable business to protect revenues, support growth and enhance customer experience. Delivered as a managed service through an expert team of experienced risk analysts, ReD Shield provides instant decisions (accept/challenge/deny) on eCommerce and mCommerce transactions. Transactions can be reviewed and recommendations acted upon using the ACI ReD Shield Customer Service Interface (CSI) application.

1.2 ACI ReD Shield ® Customer Service Interface

ACI's web-based Customer Service Interface (CSI) allows you to review detailed transaction information, use that data to create new Click & Block (C&B) rules, and disposition transactions. The C&B rules you create in CSI help ReD Shield make more accurate fraud detection recommendations going forward.

1.3 Case Manager

ACI's optional Case Manager (CM) resides within CSI, and groups like transactions into queues. Queues allow teams of Analysts to review, research, and act upon transactions without risking duplication of effort.

With Case Manager, you can note the results of your research in a particular transaction, and disposition each transaction as Approve, Pending, Cancel, or Transfer to a manager for review.

If enabled, the Tieback feature of Case Manager will automatically send each Approve and Cancel command, and research notes, to a URL (provided by the merchant or PSP) to integrate the decision with your native systems.

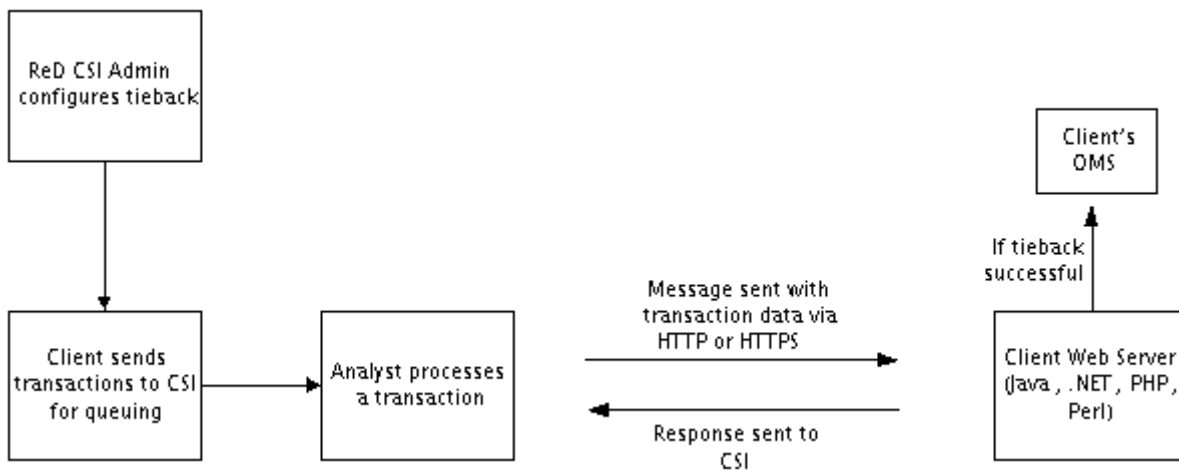
Case Manager also allows Administrators to set up Auto Analysts that automatically process transactions, that meet specified criteria, at scheduled times.

2. Tieback

Tieback is the message sent by ACI upon the Analyst reviewing a transaction and making the decision on the transaction. The message sent to the merchant/PSP ties the decision back to the native system and allows an order to be cancelled or fulfilled accordingly.

The tieback message is sent via HTTP or HTTPS to the merchant/PSP's web server.

2.1 Tieback High Level Process Flow



3. Implementing Tieback

In order to setup tieback the merchant/PSP needs to do the following:

- Request Case Manager and Tieback.
- Provide ACI with a destination URL that can receive HTTP or HTTPS POST messages.

Note: Up to three URLs can be provided but only one can be active at a time
If a non-standard port (other than 80 for HTTP or 443 for HTTPS) needs to be used, ACI must be provided with the IP address and port that the URL resolves to.

- Ensure your Content-Type header is set to `application/x-www-form-urlencoded`
- Provide the optional tieback header that ACI needs to send in the POST message

Note: All standard headers will be received in addition to these user-defined headers

- Communicating which keys (fields) to pass in the tieback request
- Provide the time in minutes (up to 5) the ACI system will wait before retrying a failed tieback message and the number of retries (up to 5)
- Provide a list of HTTP responses you will respond with

Once the initial implementation is complete, ACI will give you access to Case Manager and you can send transactions to CSI, which will then be queued. Next, you must test Tieback. For more information, see *Client Testing* on page 9.

3.1 HTTP Messaging

The tieback system uses the HTTP 1.1 protocol to send messages. Specifically the tieback system makes use of the Expect header field to allow client systems to confirm that they are expecting the tieback message. Please see RFC7231 for further details (<https://tools.ietf.org/html/rfc7231#section-5.1.1>)

The specific implementation used by ACI will send a message just containing the HTTP headers containing the with the header line "Expect: 100-continue". It then waits for either a 100 (Continue) response or an error response which your system is expected to provide. See the example header given below.

Amongst the requirements given in RFC7231 it is stated that:

"A client that sends a 100-continue expectation is not required to wait for any specific length of time; such a client MAY proceed to send the message body even if it has not yet received a response. Furthermore, since 100 (Continue) responses cannot be sent through an HTTP/1.0 intermediary, such a client SHOULD NOT wait for an indefinite period before sending the message body."

The ACI system will therefore wait for approximately one second for a response and will then send the HTTP message body if no response is received. Obviously this will introduce a delay to the messages sent so the sending of a 100-continue response is the recommended implementation.

4. Creating the Tieback Message Request

The Tieback Message Request is made up of an HTTP POST message which includes standard headers (ContentLength, Content-Type, Host, Connection, User-Agent, and Expect), optional user-defined headers, and a custom message body.

The message body contains transaction-related data that the Client requests. A typical message body in a Tieback Request is in the format Client key= ReD value. All key/value pairs are delimited by an ampersand. You must provide your keys to ACI. For example, if your key for Transaction ID is TID, you must let ACI know this so that the message can be created as you expect.

4.1 Tieback Keys

For nearly every key that you can send in a transaction, ACI can send the associated value back to you in Tieback. Some examples of keys that you might want to receive are: TransactionID, ClientID, SubClientID, Decision, CancelCode, Notes, ProcessbyUserID and ProcessDateTime.

You can also include your own Client-specific data, such as username and password. To do this, provide the key/value pair to your ReD contact and it will be appended to your Tieback message body, as shown (in blue) in the example below.

```
client=000000&subclientid=100001&transactionid=ABC123&acitransactionid=000000100  
001ABC20160914090137168&decision=CANCEL&userid=ANUser&cancelreason=216&note=lore  
m+ipsum&processdate=2016-09-14 13:00:00.000&password=NX436T&username=test1
```

4.2 Sample Tieback Message Request

The following is a sample tieback message request:

Start of POST message:

```
POST /CallbackRequestSvc/v4.0/CallBackRequestService.svc HTTP/1.1
```

Standard header:

```
Content-Length: 221  
Content-Type: application/x-www-form-urlencoded  
Host: qa.redworldwide.com  
Connection: Keep-Alive  
User-Agent: Apache-HttpClient/4.0 (java 1.5)  
Expect: 100-Continue
```

Message body:

```
client=000000&subclientid=100001&transactionid=ABC123&acitransactionid=000000100  
001ABC20160914090137168&decision=CANCEL&userid=ANUser&cancelreason=216&note=Lore  
m+ipsum+dolor+sit+amet&processdate=2016-09-14+13%3A00%3A00.0
```

4.3 Sample Message Content

Note: Not all keys will be returned in your message. For example, in the Approve message, there is no cancel reason, since the transaction was approved and not cancelled and therefore the cancelreason key will not be returned.

4.3.1 Approve

```
client=0000000&subclientid=100001&transactionid=ABC123&acitransactionid=000000100001ABC20160914090137168&decision=APPROVE&userid=ANUser&note=Lorem+ipsum+dolor+sit+amet&processdate=2016-09-14 13:00:00.000
```

4.3.2 Cancel

```
client=0000000&subclientid=100001&transactionid=ABC123&acitransactionid=000000100001ABC20160914090137168&decision=CANCEL&userid=ANUser&cancelreason=216&note=Lorem+ipsum+dolor+sit+amet&processdate=2016-09-14 13:00:00.000
```

4.3.3 Pend

```
client=0000000&subclientid=100001&transactionid=ABC123&acitransactionid=000000100001ABC20160914090137168&decision=PENDING&userid=ANUser&note=Lorem+ipsum+dolor+sit+amet&processdate=2016-09-14 13:00:00.000
```

5. Response

You should respond to a tieback message using HTTP status codes. Populating the HTTP response body is optional. Note: Any success response should not have the response body populated.

Description	HTTP Status Code	HTTP Response Body Text	Pass/Fail
Success	200		Pass
Bad Request	400	Bad Request	Fail
Unauthorized	401	Unauthorized	Fail
Forbidden	403	Forbidden	Fail
Not Found	404	Not Found	Fail

Additional HTTP codes can be used. Please let ACI what additional codes you will send and the descriptions associated with them.

6. Client Testing

For initial testing, ACI suggest that HTTP protocol is used so that in the need for any troubleshooting, the messages being sent between ACI and the client are not encrypted and the content can be seen. Once

testing has proved the connection and message flow is successful and correct, the client can instruct ACI to change to HTTPS.

When you are ready to test Tieback, an Analyst must process a Case Manager transaction.

To process a Case Manager transaction:

1. Use a web browser to access the web address (URL) for CSI provided by ACI. The login page opens.
2. Type the Client ID, Username, and Password provided by your Administrator. Then click Login.

Note: If you enter your password incorrectly five times, your user account will lock. Contact your System Administrator to unlock your account.

3. If you have a temporary password (or if your current password has expired), the system will prompt you to change your password.
4. The first time you login, the End User Licensing Agreement (EULA) opens. If you agree, click the I accept the terms of the license agreement check box and click Accept to continue.
5. From the Navigation Bar, click Queues.
6. Select the queue you wish to view



7. Click the button to enter the transaction.

8. In the Case Manager – Take Actions area, use the Pend, or Cancel options to take action on a transaction; or, click Approve.

- If you want the transaction to be Pended (held for a specific time frame until you can review it further), either leave the default date and time shown or use the calendar picker and time drop down menu to select a date and time. The pend time will be based on your time zone, and CSI will recalculate the server's time to your time zone and add the pend time. Click the

Go button . CSI moves the transaction to the appropriate place in the queue based on the specified date and time.

- If you want to Cancel the transaction, select a reason for cancellation, and click the Go button . CSI removes the transaction from all queues.

- OR

- Click Approve to accept the transaction and release it from its holding state. The Transaction Details page for the next transaction in the queue opens automatically.

When the transaction is processed, the system immediately sends a Tieback Request (via HTTP POST), to your Web Server via a URL. This Tieback message passes the keys and values that you requested. Then your system sends a response message to CSI indicating success or failure.

CSI will wait for a response from your Web Server for each Tieback message. If the Tieback fails for any reason, the Client Administrator can view (and resubmit) the failed Tieback from the Failed Tiebacks window (for more information, see Failed Tiebacks on page 11).

7. Failed Tiebacks

The Customer Service Interface (CSI) sends transaction information to your web server when an Analyst Approves or Cancels a transaction.

When the web server receives the information, you can access the order information to integrate with other native systems. Your web server also generates a message and response code and sends it back to CSI. When a failure occurs, CSI is not able to deposit the transaction information to your web server location.

CSI attempts to send the transaction information to your web server several times before considering the data exchange a true failure.

Once CSI exhausts all attempts, the transaction appears in the Failed Tiebacks list. It is from this list that the Client Administrator can resubmit the Tieback for a one-time attempt. If the Tieback fails again, it will reappear on the Failed Tieback list. Alternatively, the Client Administrator can delete the Tieback from the list.

To resubmit a tieback message, navigate to the failure list.

Setup → View my list of queues → Failed Tiebacks

Select the transaction from the list by using the check box and then click Resubmit.

8. Cipher List

Below are the cipher's and TLS versions used by the ACI Tieback servers in production and test:

Test:



Cipher Suites

# TLS 1.2 (suites in server-preferred order)		[-]
TLS_RSA_WITH_AES_256_CBC_SHA256 (0x3d)		256
TLS_RSA_WITH_AES_256_CBC_SHA (0x35)		256
TLS_RSA_WITH_AES_128_CBC_SHA256 (0x3c)		128
TLS_RSA_WITH_AES_128_CBC_SHA (0x2f)		128
TLS_RSA_WITH_3DES_EDE_CBC_SHA (0xa)		112
TLS_RSA_WITH_RC4_128_SHA (0x5) INSECURE		128
TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384 (0xc028) ECDH secp256r1 (eq. 3072 bits RSA) FS		256
TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA (0xc014) ECDH secp256r1 (eq. 3072 bits RSA) FS		256
TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256 (0xc027) ECDH secp256r1 (eq. 3072 bits RSA) FS		128
TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA (0xc013) ECDH secp256r1 (eq. 3072 bits RSA) FS		128
TLS_ECDHE_RSA_WITH_3DES_EDE_CBC_SHA (0xc012) ECDH secp256r1 (eq. 3072 bits RSA) FS		112
# TLS 1.1 (suites in server-preferred order)		[-]
TLS_RSA_WITH_AES_256_CBC_SHA (0x35)		256
TLS_RSA_WITH_AES_128_CBC_SHA (0x2f)		128
TLS_RSA_WITH_3DES_EDE_CBC_SHA (0xa)		112
TLS_RSA_WITH_RC4_128_SHA (0x5) INSECURE		128
TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA (0xc014) ECDH secp256r1 (eq. 3072 bits RSA) FS		256
TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA (0xc013) ECDH secp256r1 (eq. 3072 bits RSA) FS		128
TLS_ECDHE_RSA_WITH_3DES_EDE_CBC_SHA (0xc012) ECDH secp256r1 (eq. 3072 bits RSA) FS		112
# TLS 1.0 (suites in server-preferred order)		[-]
TLS_RSA_WITH_AES_256_CBC_SHA (0x35)		256
TLS_RSA_WITH_AES_128_CBC_SHA (0x2f)		128
TLS_RSA_WITH_3DES_EDE_CBC_SHA (0xa)		112
TLS_RSA_WITH_RC4_128_SHA (0x5) INSECURE		128
TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA (0xc014) ECDH secp256r1 (eq. 3072 bits RSA) FS		256
TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA (0xc013) ECDH secp256r1 (eq. 3072 bits RSA) FS		128
TLS_ECDHE_RSA_WITH_3DES_EDE_CBC_SHA (0xc012) ECDH secp256r1 (eq. 3072 bits RSA) FS		112

Production:



Cipher Suites

TLS 1.2 (suites in server-preferred order)

TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384 (0xc028)	ECDH secp521r1 (eq. 15360 bits RSA) FS	256
TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256 (0xc027)	ECDH secp521r1 (eq. 15360 bits RSA) FS	128
TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA (0xc014)	ECDH secp521r1 (eq. 15360 bits RSA) FS	256
TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA (0xc013)	ECDH secp521r1 (eq. 15360 bits RSA) FS	128
TLS_RSA_WITH_AES_256_GCM_SHA384 (0x9d)		256
TLS_RSA_WITH_AES_128_GCM_SHA256 (0x9c)		128
TLS_RSA_WITH_AES_256_CBC_SHA256 (0x3d)		256
TLS_RSA_WITH_AES_128_CBC_SHA256 (0x3c)		128
TLS_RSA_WITH_AES_256_CBC_SHA (0x35)		256
TLS_RSA_WITH_AES_128_CBC_SHA (0x2f)		128

TLS 1.1 (suites in server-preferred order)

TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA (0xc014)	ECDH secp521r1 (eq. 15360 bits RSA) FS	256
TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA (0xc013)	ECDH secp521r1 (eq. 15360 bits RSA) FS	128
TLS_RSA_WITH_AES_256_CBC_SHA (0x35)		256
TLS_RSA_WITH_AES_128_CBC_SHA (0x2f)		128

TLS 1.0 (suites in server-preferred order)

TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA (0xc014)	ECDH secp521r1 (eq. 15360 bits RSA) FS	256
TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA (0xc013)	ECDH secp521r1 (eq. 15360 bits RSA) FS	128
TLS_RSA_WITH_AES_256_CBC_SHA (0x35)		256
TLS_RSA_WITH_AES_128_CBC_SHA (0x2f)		128

9. Revision History

Date	Version	Description
2014-08-15	1.0	Initial publication

2014-11-03	1.1	Added information about standard headers, a full sample tieback message request and how to process Case Manager transactions
2016-09-15	1.2	Corporate rebranding Added additional detail on how to respond to a tieback message Updated example messages
2016-10-12	1.3	Added the HTTP 1.1 messaging requirements
2017-06-14	1.4	Document format refresh Added Test and Production cipher lists
2018-01-02	1.5	Removed “202 Success” from Tieback response codes

© Copyright ACI Worldwide, Inc. 2017

ACI, ACI Worldwide, ACI Payment Systems, the ACI logo, ACI Universal Payments, UP, the UP logo, ReD, PAY.ON and all ACI product names are trademarks or registered trademarks of ACI Worldwide, Inc., or one of its subsidiaries, in the United States, other countries or both. Other parties' trademarks referenced are the property of their respective owners.