Experian Products and Services

Precise ID XML Gateway

Raw XML Method

Experian Client Services Delivery

April 22, 2016

Experian does not recommend, endorse, or support applications that manipulate the Teletype Response Format report in any form—including the Teletype Response Format report embedded in the Automated Response Format 700 segments as part of the Parallel Profile report. Only the Automated Response Format or field level XML response should be scored, reformatted or manipulated in any way. Details regarding Teletype Response Format report character positions are not made available and the report will change without notice.

Experian policy prohibits clients and vendors from exposing Experian data over the internet or any other public network without express permission from Experian. Should you or your client have a business need to expose Experian data in such a way, please contact your Experian Technical Services and Support Representative (TSSR).

Experian
475 Anton Blvd
Costa Mesa, CA 92626
800.854.7201
www.experian.com

History of Revisions

Date	Page	Description
11/14/12		First draft
05/20/14	1	Updated Important note section
	4	Updated URLs for Prod and Demo
03/12/15	12	Remove references to SSL 3.0
04/24/15	4	Update Authorization Header format
06/16/15		Update for V6 XML
09/18/15	4	Add Extranet URLs
	5	Update POST URL Move ReferenceNumber tag to correct location
	8	Add namespace to response parent tag (<Experian>)
01/07/2016	5	Add verbiage for URL used in the example
04/22/2016	3	Add certificate import information (API-109)
	4	Correct Production Extranet URL (API-114)
	9	Add XML Gateway error codes/descriptions
		Create Active-Active version

This page intentionally left blank

Contents

This page intentionally left blank

Precise ID XML Gateway

Important Note

Once you have completed your Precise ID XML Gateway coding the following must be met:

1. Experian must certify your work to ensure that it meets our security requirements ***before you are allowed access to our production environment***. Please contact your TSSR Representative for more information on the certification process.
2. Any company that is not a direct subscriber of Experian and takes possession of data provided by Experian on behalf of an Experian subscriber is considered a 3rd party processor and is required to complete an Experian Independent 3rd Party Assessment (EI3PA) if its customers connect to them over a public network, such as the Internet. Possession of data can be for a prescribed time frame or as a simple pass-through.

Product Summary

Precise ID XML Gateway is a business-to-business application gateway that allows access to Experian's Fraud & Identity Solutions systems via the public Internet or Experian's private TCP/IP extranet transport. It is a secure 2048-bit encrypted transaction, using HTTPS. Precise ID XML Gateway is a non-browser-based system requiring Experian-certified client or vendor software at the user's location. It utilizes XML for the input inquiry and returns field-level XML.

Precise ID XML Gateway meets the encryption standards requirement in the Safeguards section of the Gramm-Leach-Bliley (GLB) Act.

Precise ID XML Gateway includes:

- A service to determine the correct URL for accessing Precise ID XML Gateway
- Support for Experian's Single Sign-On (SSO) service
- for XML inquiries and response

Clients with "hard wired" connectivity to the Internet have the benefits of a leased line at a fraction of the cost.

There are no monthly volume requirements or connectivity costs for this solution.

Terms and Definitions

The following is a list of terms and definitions used in this document.

Term	Definition
User ID	The Single Sign-On User ID assigned to each client for access to Precise ID XML Gateway. This ID must be protected and not available for users to view. The User ID cannot be less than 6 characters or longer than 32 characters and cannot contain most special characters (e.g., @, *, &, etc.). User IDs are free form and can be a combination of alpha and numeric characters. Experian recommends that user's adopt the same user ID issuance pattern that is standard at their place of business.
Password	The unique password associated with the Precise ID XML Gateway user ID. It must be protected and not available for users to view. Passwords must be a minimum of 8 characters and a maximum of 32. The password must contain at least one numeric character. Some general recommendations when creating a password: DO NOT create a password with consecutive digits (e.g., 123456) or repeated characters (e.g., aaabbb). 1. DO NOT create cyclical passwords (e.g., d42jan, d42feb, etc.) 2. DO NOT create passwords that can be easily guessed (e.g., your spouse's name, names of children, pets, etc.). 3. DO NOT create passwords that pertain to your personal interests (e.g., favorite sports team, things you collect, vintage cars, etc.). 4. DO NOT create passwords that are words found in the dictionary (including foreign words). 5. Passwords should not be the same or similar as your User ID. Do not repeat your passwords for at least 18 iterations.
Reference Number	This optional value is designed to allow the Client application to match the inquiry with the response. The data is not processed or used by Experian, and is returned in the <ReferenceNumber> </ReferenceNumber> element in the response.
Completion Code	This value determines a successful transaction or an error
Host Response	The response returned from the Experian system. The output is identical to the existing format.

Features

The following features are available through the XML Gateway facility:

- It is a secure 2048-bit encrypted transaction, using HTTPS.
- It is a non-browser-based system requiring an intelligent client at the user's location.
- It incorporates a service to determine the URL for the appropriate version of Precise ID XML Gateway
- It contains support for Experian's Single Sign-On (SSO)
- It supports XML inquiries

Getting Started

The topics contained in this section are intended to provide developers the steps to be undertaken in order to successfully develop and test client applications accessing Precise ID XML Gateway.

Prerequisites

The developer who will be executing the steps in this section is assumed to meet the following prerequisites:

1. Working knowledge and experience with XML
2. Experience in programming languages which support HTTPS Post, such as Java and .Net.
    a. Go to https://pks.experian.com
    b. Download the "Public Certificate for the Primary CA"
    c. Download the "Public Certificate for the Sub CA"
    ~~a.~~d. Import these certificates into your security stor using the appropriate process

User ID and Password

An authorized user of Precise ID XML Gateway is also granted access to Precise ID Web UI via eSolutions. A new user is assigned a temporary password which must be changed by the user after logging in to eSolutions for the first time.

The following steps shall be executed by the user for the first time in order to verify access to Precise ID and change the temporary password:

1. Login to Experian's eSolutions using the following URL:

    https://www.experian.com/esolutions/

2. Enter Username and Password.
3. The following message will be displayed if the Username or Password is not valid:

    "The username or password is invalid. Please check the information and try again. If you are still having problems, consult with your designate or contact Experian Technical Support 800-854-7201."

4. If the Username and Password are valid, the user is required to change the password and confirm other information if the user has logged in for the first time.
5. Change the password and confirm other information.
6. Login to eSolutions again using the following URL to verify access using the new password:

    https://www.experian.com/esolutions/

Migrating from Net Connect to XML Gateway

The following steps must be completed in order to successfully migrate from Net Connect to XML Gateway:

1. Change URL from the Net Connect URL to the XML Gateway URL (URLs are specified in a later section).
2. Remove call to ECALS, if applicable (only one call is required for XML Gateway).

Functional Requirements

The following is a list of the functional requirements for using the Precise ID XML Gateway channel:

Transaction Flow Summary

The Precise ID XML Gateway client session can be summarized as follows.

1. Precise ID XML Gateway client connects to the specified URL.

   Demo (Internet): https://dm-sgw1.experian.com/fraudsolutions/xmlgateway/preciseid

   Production (Internet): https://pid-sgw.secure.experian.com/fraudsolutions/xmlgateway/preciseid

   Precise ID XML Gateway client sends HTTPS POST transaction containing consumer data.

2. Precise ID XML Gateway client receives Experian response.

Migrating from Form Post to Raw XML

For those clients migrating from the legacy Net Connect or Form Post XML Gateway access methods, the following items are required for the Raw XML XML Gateway method:

1. Ensure that the following header is submitted: "Content-Type: text/xml
2. Remove the "NETCONNECT_TRANSACTION" form post key parameter
3. Do not URL-encode the XML payload

HTTPS POST Request Format

The XML request is sent to Precise ID XML Gateway using the HTTPS POST request method. The HTTPS request must contain the following elements (refer to the example below for a sample POST):

Headers

Authorization

The User ID and Password (see section Authentication Requirements for more information) are sent in the Authorization header. The content of the header is:

Basic userid:password

Note: The "userid:password" value (including the colon) must be Base64 encoded.

Content-Type

text/xml

Content-Length

The length of the XML payload.

Note: Transaction problems (excessive timeouts, duplicate transactions, etc.) can occur if your HTTPS request contains our ClearTrust session cookie. Therefore, we recommend that you DO NOT return it in the HTTPS request header on subsequent transactions. Some plug-ins may do this automatically, so please check and make the necessary arrangements to deactivate it.

Content

The content of the POST request contains the raw xml payload of the request itself. The payload must be properly formatted and encoded according to XML standards. The content-type in the http header should be set to text/xml.

HTTPS POST Example

The following is an example of a dump of the HTTPS POST transaction through the Demo (Internet) URL:

```
POST:  https://dm-sgw1.experian.com/fraudsolutions/xmlgateway/preciseid HTTP/1.1
Content-Type:  text/xml
Authorization:  Basic YTAxATMxYV9waWQ6UGFzc3dvedA1
Content-Length:  1094

<?xml version="1.0" encoding="UTF-8"?>
<Experian>
  <FraudSolutions>
     <Request>
       <Products>
         <PreciseIDServer>
           <PIDXMLVersion>06.00</PIDXMLVersion>
           <Subscriber>
             <Preamble>TCA1</Preamble>
             <OpInitials>SG</OpInitials>
             <SubCode>1429010</SubCode>
           </Subscriber>
           <PrimaryApplicant>
             <Name>
               <Surname>STANLEY</Surname>
               <First>ROGER</First>
               <Middle>D</Middle>
               <Gen/>
             </Name>
             <SSN>666542396</SSN>
             <CurrentAddress>
               <Street>100 50TH ST SW APT 125</Street>
               <City>GRAND RAPIDS</City>
               <State>MI</State>
               <Zip>49548</Zip>
             </CurrentAddress>
             <DriverLicense>
               <State>MI</State>
               <Number>S550792603937</Number>
             </DriverLicense>
             <Phones>
               <Phone>
                 <Number>6165311574</Number>
                 <Type/>
               </Phone>
             </Phones>
             <DOB>12091949</DOB>
           </PrimaryApplicant>
           <Verbose>Y</Verbose>
           <Options>
             <ReferenceNumber>12345</ReferenceNumber>
             <ProductOption>06</ProductOption>
```

```
            <DetailRequest>D</DetailRequest>
          </Options>
        </PreciseIDServer>
      </Products>
    </Request>
  </FraudSolutions>
</Experian>
```

HTTP Response

HTTP Response Codes

The following are the most common HTTP response codes:

HTTP Status Code	Explanation	Action
200 – OK	Successful authentication. Transaction reached the Precise ID XML Gateway application successfully.	No action required
401 – Unauthorized	Any of the following: Unauthorized user (this can occur due to an incorrect User ID and/or Password); incorrect base64 encoding in the authorization header; client did not open SSL socket/not using HTTPS; MTU needs to be changed to 1492.	Correct the User ID or password or your base64 encoding.
403 – Forbidden	Transaction was authenticated but not authorized. The user ID may not have access to Precise ID XML Gateway product or it may be locked due to too many password violations.	Contact your TSSR
500 – Server Unavailable	Precise ID XML Gateway application is unavailable or the url specified is incorrect.	Contact your TSSR

HTTP Response Headers

The following headers will be returned for response codes 200, 403 and 404:

- Status Line
- Server
- Date
- Set-cookie (contains the cookie)
- Content-length
- Content-type
- Connection

The following headers will be returned for response code 401:

- Status Line
- Server
- Date
- Location
- Connection

Request Format

Request Header Tags

The Precise ID XML Gateway request begins with the `<Experian>` parent tag. The table below describes the Request Header tags to be submitted with every inquiry to Precise ID XML Gateway.

Tag	Req.	Data Type	Max Len.	Description (Keyword)
Experian	Y			Start tag for Experian request elements
FraudSolutions	Y			Start tag for Fraud Solutions request elements
Request	Y			Start tag for Request elements
Products	Y			Start tag for Products elements
PreciseIDServer	Y			Start tag for Precise ID Server elements
PreciseIDServer tags	Y	Var	Var	Precise ID Server-specific request tags. Refer to the appropriate Precise ID product option API for more information.
/PreciseIDServer	Y			End tag for Precise ID Server elements
/Products	Y			End tag for Products elements
/Request	Y			End tag for Request elements
/FraudSolutions	Y			End tag for Fraud Solutions request elements
/Experian	Y			End tag for Experian request elements

Request Example

The following is an example of a Precise ID XML Gateway request:

```
<?xml version="1.0" encoding="UTF-8"?>
<Experian>
  <FraudSolutions>
     <Request>
       <Products>
         <PreciseIDServer>
              .
              .
                 Refer to the appropriate Precise ID product option API for more information
              .
              .
         </PreciseIDServer>
       </Products>
     </Request>
  </FraudSolutions>
</Experian>
```

Response Format

Response Header Tags

The Precise ID XML Gateway response begins with the <Experian> parent tag. The response format is used for successfully processed transactions (Completion Code = 0000). The table below provides a description of the Response Header tags.

Tag	Data Type	Max Length	Description
Experian			Start tag for Experian response elements
FraudSolutions			Start tag for Fraud Solutions response elements
Response			Start tag for Response elements
Products			Start tag for Products elements
PreciseIDServer			Start tag for Precise ID Server elements
PreciseIDServer tags			Precise ID Server-specific response tags. Refer to the appropriate Precise ID product option API for more information.
/PreciseIDServer			End tag for Precise ID Server elements
/Products			End tag for Products elements
/Response			End tag for Response elements
/FraudSolutions			End tag for Fraud Solutions response elements
/Experian			End tag for Experian response elements

Response Example

The following is an example of a Precise ID XML Gateway response:

```
<?xml version="1.0" encoding="UTF-8"?>
<Experian xmlns="http://www.experian.com/NetConnectResponse">
  <FraudSolutions>
     <Response>
       <Products>
         <PreciseIDServer>
              .
              .
                 Refer to the appropriate Precise ID product option API for more information
              .
              .
         </PreciseIDServer>
       </Products>
     </Response>
  </FraudSolutions>
</Experian>
```

Error Format

Error Header Tags

The Precise ID XML Gateway error response begins with the <NetConnectResponse> parent tag. Note that this is different from the root tag for a successful response. This response format is used for unsuccessfully processed transactions (Completion Code ≠ 0000). The table below provides a description of the Error Header tags.

Tag	Data Type	Max Length	Description
NetConnectResponse			Start tag for NetConnect Response elements
CompletionCode			XML Gateway Completion Code and Error Message: "1000" Invalid request format "4000" System error
ErrorMessage			
ReferenceID			Echo back from the ReferenceID tag in the request. Allows client application to match request with response.
/NetConnectResponse			End tag for NetConnect Response elements

Error Example 1

The following is an example of an error response where a system error occurred.

```
<?xml version="1.0" standalone="no"?>
<NetConnectResponse>
  <CompletionCode>4000</CompletionCode>
  <ErrorMessage> System error. Call Experian Technical Support at 1-800-854-
    7201.</ErrorMessage>
  <ReferenceId>userabc001</ReferenceId>
</NetConnectResponse>
```

Error Example 2

The following is an example of an error response where the request XML is not properly formatted.

```
<?xml version="1.0" standalone="no"?>
<NetConnectResponse>
  <CompletionCode>1000</CompletionCode>
  <ErrorMessage>Invalid Request Format</ErrorMessage>
</NetConnectResponse>
```

Password Maintenance

Password Guidelines

The password automatically expires ninety days after its creation after which access is denied. Therefore, users must regularly change their password in order to maintain continuous service.

Production users will receive a password email reminder approximately ten days prior to the expiration of a password. The email will be sent to the email address associated with User ID, so it is very important that the email address be kept up to date in our Access Control System.

Since development and testing of a Precise ID XML Gateway application normally take less than ninety days, staging (test) users will not receive an email reminder. It is up to them to remember to maintain their testing password.

Passwords can be either manually changed using the appropriate Experian web site or they can be programmatically changed using the Automated Password Reset Function (see the "Automated Password Reset Function" section below for details).

If the Automated password reset function is not used, then the user's Precise ID XML Gateway application should remind users to change their password at regular intervals prior to its expiration. This is a requirement for third-party software applications.

To manually change the password, use the following URLs:

Demo (Internet): https://dm2.experian.com/securecontrol/reset/profilelogon.jsp
Demo (Extranet): https://dm1.experiannet.com/securecontrol/reset/profilelogon.jsp
Production (Internet): https://ss3.experian.com/securecontrol/reset/profilelogon.jsp
Production (Extranet): https://www.experiannet.com/securecontrol/reset/profilelogon.jsp

If the software normally changes passwords programmatically and a manual password change is made, then the software must automatically change the password again once it is aware of the new password. This is a requirement for Precise ID XML Gateway certification.

Password Expiration

Recommendation: If not automatically changed by the software, the Precise ID XML Gateway software should track the number of days since the supervisor last changed the Precise ID XML Gateway password. Beginning about the 80th day, the software should begin to remind the supervisor to change their Precise ID XML Gateway password (both at Experian and within the software). By the 85th day the software should remind the supervisor that failure to change the Precise ID XML Gateway password will result in interruption of service. This message will continue until the supervisor changes the password.

Recommendation: When manually changing the password, the software should ask the supervisor to commit it to memory.

Recommendation: It is recommended that the software notify any logged in user at the time the Precise ID XML Gateway password expires. The user should be directed to notify the system administrator to log in and change the password.

Recommendation: It is also recommended that when the administrator logs into the software after the Precise ID XML Gateway password expires that a message should display stating that the Precise ID XML Gateway password has expired and it should contain a link to the Experian authentication system's URL.

Automated Password Reset Function

An Automated Password Reset Function is available for those who want to programmatically change the password. It uses an HTTPS POST to the following URLs.

Automated Password Reset URLs

To automatically change the password, use the following URLs:

Internet access:
Production and Demo: https://ss3.experian.com/securecontrol/reset/passwordreset

Extranet (VPN / leased line):
Production and Demo: https://www.experiannet.com/securecontrol/reset/passwordreset

Automated Password Reset Pre-Conditions

The following conditions must be met before the automated password reset process can be used:

- The current user ID and password must be active. If no user ID exists, one must be manually created.
- The Precise ID XML Gateway client must use an HTTPS connection.
- The Precise ID XML Gateway client must connect to the Automated Password Reset function using a fully-qualified static IP address. If not, the user will receive an HTTP status code of "401 Unable to authenticate response."

  Test/Staging: Contact your TSSR to have your IP address(es) added to your User ID. A maximum of ten IP addresses may be added. Address ranges may also be used.

  Production: The client's Head Designate must contact the Fraud Business Implementation Specialist to have the IP address(es) added to your User ID. Up to ten IP addresses or address ranges can be added.

  Note: Adding IP addresses to the User ID restricts usage to only those IP addresses for *all* transactions, so make sure that you also add the ones for your normal transaction processing if they are different.

- The Precise ID XML Gateway client should have a property that states the frequency at which it wants to do a password reset. The recommended frequency is 30 days, not to exceed 45 days. Every time the client runs, it should check the date it last did a password reset. If it has been more than the specified number of days, then the automated password reset process is run. If not, it carries out its normal transaction processing.

Automated Password Reset Process Flow

The Automated password reset function includes two HTTPS POST transactions. The process consists of the following steps:

1. **Request new password**: The Precise ID XML Gateway client connects to Experian using an HTTPS POST and Basic authentication to indicate that it is requesting a new password. The client passes the user ID and current password in the same manner as in a normal Precise ID XML Gateway transaction. It also passes the following key value pairs:

   ```
   "command=requestnewpassword"
   "application=xmlgateway".
   ```

   A dump of the HTTPS POST would look similar to this:

   ```
   POST /securecontrol/reset/passwordreset HTTP/1.1
   Authorization: Basic dGVzdGlkOnBhc3N3b3Jk
   Content-Type: application/x-www-form-urlencoded
   Cache-Control: no-cache
   Host: ss3.experian.com
   Connection: keep-alive
   Content-Length: 51

   &command=requestnewpassword&application=xmlgateway
   ```

2. **Receive new password**: The Precise ID XML Gateway client receives the new password in the Experian response. The client can store this password so that it can be retrieved later. Please note that the password has not been reset yet. A dump of the response would look similar to this:

   ```
   HTTP/1.1 200 OK
   Date: Tue, 09 Mar 2010 22:29:02 GMT
   Content-type: text/plain
   Set-Cookie: EntlogonWebAppSession=E2C.....
   Cache-control: no-cache="set-cookie"
   Response: XXXXXXXXX
   ```

3. **Reset password**: The Precise ID XML Gateway client connects to Experian again using an HTTPS POST and Basic authentication to indicate that it is requesting a password reset. The client must authenticate again using the existing user ID and password and passes the following key value pairs in the transaction:

   "newpassword=XXXXXXXXX(password received in step 2 in clear text)
   "command=resetpassword"
   "application=xmlgateway"

   A dump of the HTTPS POST would look similar to this:

   ```
   POST /securecontrol/reset/passwordreset HTTP/1.1
   Authorization: Basic dGVzdGlkOnBhc3N3b3Jk
   Content-Type: application/x-www-form-urlencoded
   Host: ss3.experian.com
   Content-Length: 67

   &newpassword=XXXXXXXXX&command=resetpassword&application=xmlgateway
   ```

4. **Receive the status**: The client receives the status of the password reset request as a string in the response. If the reset was successful the sting value is "SUCCESS". In any other scenario, the status string will have an error message explaining the error (see Automated Password Reset Errors section below for errors).

   ```
   HTTP/1.1 200 OK
   Date: Tue, 09 Mar 2010 22:31:02 GMT
   Content-Type: text/plain
   Set-Cookie: EntlogonWebAppSession=Lh1b....; path=/
   Transfer-Encoding: chunked
   Response: SUCCESS
   ```

5. **Save password**: If the status string is "SUCCESS", the client saves the new password and uses this password to login to Precise ID XML Gateway.

Automated Password Reset Errors

The response string will have an error message if the process is not successful. The most common is an authentication failure, which will appear similar to this example:

```
HTTP/1.1 401 Moved Temporarily
Date: Tue, 09 Mar 2010 22:31:02 GMT
Content-Type: text/plain
Set-Cookie: EntlogonWebAppSession=Lh1bL....; path=/
Response: Unable to authenticate
```

Status Code	Response Text	Reason
400	Invalid Input	Input parameter is missing or invalid
401	Unable to authenticate	Invalid user ID/password
500	Application Error	Contact your TSSR

This page intentionally left blank