
Credit card security requirements

What's changing

As one step in our continual efforts to enhance security for our partners and customers, we will be requiring our API resellers to submit credit card information securely.

When the change goes into effect

In our production system, resellers may pass credit card information through the secure environment at any time, but will be **required** to do so beginning **June 15, 2010**.

Starting June 15, API queries that contain credit card information will fail if they are not submitted through the secure environment.

In our test system, we will enforce the change beginning **April 15, 2010**.

Circumstances under which this change applies

When you use the eNom API to pass credit card information, you **must** use a secure connection. Such information includes not only the credit card number, but also CVV2, expiration date, cardholder name, and address information.

When commands do not contain credit card information, use of the secure environment is optional.

How to implement our credit card security requirements

API queries that include credit card information should be submitted using secure (**https**) protocol.

Production system: **<https://reseller.enom.com/interface.asp?QueryString>**

Test system: **<https://resellertest.enom.com/interface.asp?QueryString>**

API commands to which this applies

When you submit any of the following API commands with credit card information in the query string, you must do so with a secure connection.

- **CreateAccount**
- **Extend**
- **ExtendDomainDNS**
- **Purchase**
- **PurchaseHosting**
- **PurchaseServices**
- **RefillAccount**
- **RenewPOPBundle**
- **RenewServices**
- **TP_CreateOrder**
- **TP_SubmitOrder**
- **UpdateAccountInfo**