

ShopSite Knowledgebase

February 16, 2016 email from Authorize.net regarding 'Technical Updates' (Akamai, Transaction IDs, RC4, TLS)

Product: ALL
Version: ALL
Platform: ALL

I received an email notification from Authorize.net summarizing 4 upcoming changes to their services. Do these affect my ShopSite? Is there anything that I need to do?

How the four listed issues may affect ShopSite stores are as follows:

1. Akamai SureRoute Reminder - ShopSite has tested against Authorize.Net's Phase 1 new transaction URLs that are already using the Akamai system and have not encountered any problems. We do not anticipate any issues when Authorize.net switches their current production URLs over in June 2016, and because they are moving over the existing URLs automatically, no changes will need to be made to ShopSite settings for that switchover to occur.

NOTE: While ShopSite doesn't have any restrictions on IP addresses, it is possible that your hosting provider only allows outgoing connections to specific IP addresses, so you would need to contact them to see if they have any such firewall restrictions and make sure the new Akamai servers are in their allowed list.

2. Transaction and Batch ID Reminder - ShopSite does not have restrictions on the length of Authorize.net Transaction IDs or require that they be sequential so this does not apply.

3. RC4 Cipher Disablement - ShopSite does not rely on RC4 ciphers so this does not apply.

4. TLS Remediation for PCI DSS Compliance - ShopSite 12 sp2 r4 added TLS 1.1 and 1.2 connection capabilities, so this does not apply to merchants using this version of ShopSite or newer. If you are using an older version of ShopSite this will become an issue for you sometime in 2017 when Authorize.net disables TLS 1.0 unless you upgrade your ShopSite to 12 sp2 r4 or higher before then. Contact your hosting provider or ShopSite reseller regarding upgrading your version of ShopSite if necessary.

The 2/16/2016 email sent to merchants by Authorize.net is as follows:

Subject: Authorize.Net Technical Updates

Your Payment Gateway ID:

Dear Authorize.Net Merchant:

Over the next few months, we are making several updates to our systems that you need to be aware of. They are all technical in nature and may require the assistance of your web developer or shopping cart/payment solution provider.

Please read this email carefully, and if you need to find a web developer to help you, please check out our Certified Developer Directory at www.authorize.net/cdd.

Akamai SureRoute Reminder

As we get further into 2016, we want to remind you of our previously announced Akamai SureRoute implementation plan and timelines. Using Akamai's technology will help safeguard against interruptions caused by issues beyond our direct control, such as Internet congestion, fiber cable cuts and other similar issues.

If you have not already, please review the announcement and the Akamai FAQs to determine what action you should take for your particular solution. If your solution uses a firewall, please pay particular attention to this section of the FAQs to make sure you avoid any disruptions to your transaction processing.

Transaction and Batch ID Reminder

In the coming months, due to system updates, it will be possible to receive Authorize.Net IDs (Transaction ID, Batch ID, etc.) that are not in sequential order.

For example, currently, if you receive a Transaction ID of "1000," you could expect that the next Transaction ID would not be less than 1000. However, after the updates, it will be possible to receive a Transaction ID less than the one previously received.

If your system has any functionality that expects Authorize.Net-generated IDs to be sequential, please update it immediately so that you will not see any disruptions.

Additionally, please make sure that your solution does not restrict any Authorize.Net ID field to 10 characters. If you are required to define a character limit when storing any of our IDs, the limit should be no less than 20 characters.

RC4 Cipher Disablement

In an effort to ensure that all of your server-to-server communications with the Authorize.Net platform (both transactional and otherwise) maintain the highest levels of security, we will be disabling the RC4 cipher suite during the first half of 2016. A follow-up notification will be sent out once specific dates for the disablement are ready for the sandbox and production environments.

For now, if you have a solution that relies on RC4 to communicate with our servers, please update it to a current, high-security cipher as soon as possible. Please review our API best practices blog post for more information.

TLS Remediation for PCI DSS Compliance

As you may already be aware, new PCI DSS requirements state that all payment systems must disable TLS 1.0 by 2018. Though we are still finalizing our plans for remediating TLS 1.0 in both sandbox and production, we will be disabling TLS 1.0 in sandbox and production in early 2017. This is to ensure that we are compliant ahead of the PCI date.

In addition, we are discussing the possibility of disabling TLS 1.1 at the same time, because while it is not expressly forbidden, there are enough concerns surrounding it. TLS 1.2 is currently the strongest available protocol, and we strongly urge all merchants and developer partners to use it for their API integrations.

For more information, including updates to the dates we anticipate disabling TLS in each environment, please refer to our previous blog post.

Sincerely,
Authorize.Net

