Merchant security

System upgrade guide

Click HERE for information on SHA-256 compliance.

Help future-proof your integration.

Global security threats are constantly changing and the security of our merchants continues to be our highest priority. To guard against current and future threats, we're encouraging you to make the following upgrades to your integrations:

1. Discontinue use of the VeriSign G2 Root Certificate
2. Update your integration to support certificates using the SHA-256 algorithm

Why change?

The public Certificate Authority (CA) industry continues to improve the security of SSL certificates. In preparation for requiring the use of the SHA-256 signing algorithm in 2016, the VeriSign G2 Root Certificate will no longer be supported. This certificate was historically used for connecting to PayPal API and Instant Payment Notification (IPN) endpoints.

When do I need to act?

We recommend that you act as soon as possible to prepare for these changes. For a detailed timeline, including upgrade dates for Live and Sandbox API endpoints, see our 2015-2016 SSL Certificate Change microsite.

NOTE: These changes are to address industry-wide security issues and are not unique to PayPal. When implemented, they'll improve the privacy and reliability of your PayPal integrations. Because the details of these changes vary by system, we recommend they be made with the help of a qualified system administrator.

1. Discontinue use of the VeriSign G2 Root Certificate

The issue: In the past, VeriSign issued SSL certificates that had a trust chain signed by a 1024-bit G2 Root Certificate. In recent years, the US government and Public CA industry have moved to more secure 2048-bit certificates, so VeriSign now issues SSL certificates that have a trust chain signed by a 2048-bit G5 Root Certificate issued in 2006.

Our response: In accordance with industry standards, we won't continue to accept secure connections to the API/IPN endpoints that expect our certificate/trust chain to be signed by the G2 Root Certificate. Only secure connection requests that expect our certificate/trust chain to be signed by the G5 Root Certificate will result in successful secure connections.

What you must do…

If your system currently mandates the use of the VeriSign Root Certificate, you must discontinue use of SSL connections that rely on the certificate with a G2 identifier. The industry is actively working to phase out 1024-bit Root Certificates this year.

- Secure connections that rely on our certificate chain being signed by the G2 Root Certificate are not supported:

Organisational unit	Class 3 Public Primary Certification Authority - **G2**
Serial number	7d d9 fe 07 cf a8 1e b7 10 79 67 fb a7 89 34 c6
Certificate SHA1 fingerprint	85 37 1c a6 e5 50 14 3d ce 28 03 47 1b de 3a 09 e8 f8 77 0f

- Secure connections that rely on our certificate chain being signed by the G5 Root Certificate are supported:

Common Name	VeriSign Class 3 Public Primary Certification Authority - **G5**
Serial Number	18 da d1 9e 26 7d e8 bb 4a 21 58 cd cc 6b 3b 4a
Certificate SHA1 Fingerprint	4e b6 d5 78 49 9b 1c cf 5f 58 1e ad 56 be 3d 9b 67 44 a5 e5

Follow these guidelines to ensure you're securely connecting using a supported VeriSign G5 Root Certificate:

1. **Check your certificate store.** Ask your website host or system administrator to verify that the VeriSign G5 Root Certificate is included in the root store being used by your code for validation logic. If it is, no action is required.
    - See the following links to check your keystore for the presence of the G5 Root Certificate using Java, Linux or Windows.

2. **Check your error logs.** If the VeriSign G5 Root Certificate has not been downloaded to replace the G2 Root Certificate, you may see error messages like:
    - SSL handshake error, "No trusted certificate found"
    - Result code -31, "The certificate chain did not validate, no local certificate found"
    - Result code -8, "SSL connection failed"
    - -1 error

    To resolve these issues, either:

    - Update your software to the latest version that supports SHA-256, or
    - If a keystore is used for certificate validation/authentication, install the VeriSign G5 Root Certificate into your keystore.

3. **Obtain a VeriSign G5 Root Certificate.** If your certificate store or Java client does not include the VeriSign G5 Root Certificate, ask your system administrator to download it from VeriSign and save it in the certificate store, as well as any other SSL connection authentication packages.
    - Download Symantec's VeriSign G5 Root Certificate
    - Download specific server SSL certificates, if required by your server

2. Update to the SHA-256 signing algorithm

The issue: SHA-1 is a 22-year-old cryptographic algorithm that is being threatened by increases in computing power. SHA-256 uses a stronger algorithm with 256-bit hash values.

Our response: We're upgrading SSL certificates on all Live and Sandbox endpoints from SHA-1 to the stronger and more robust SHA-256 in mid-2016.

What you must do…

Follow these guidelines to transition from using SSL certificates that utilise the SHA-1 signing algorithm to the stronger SHA-256 signing algorithm:

1. **Check your environment.** Ensure that your environment supports SHA-256 certificates.
    - Refer to online resources, such as DigiCert's SHA-2 Compatibility Guide and Symantec's Supported Browser and Server List, for a list of supported hardware and software.
    - If parts of your environment do not support SHA-256, you'll need to replace or upgrade those pieces before you can implement the new certificates.
    - Windows 2000 Server and some versions of Windows XP may be incompatible with SHA-2. This Windows PKI blog on SHA2 and Windows can assist with patches and recommendations to upgrade your environment.
2. **Check your certificates.** If your environment supports SHA-256, ensure you have the VeriSign G5 Root Certificate in your keystore.

Questions?

For additional details and frequently asked questions, please see our 2015-2016 SSL Certificate Change microsite.