OPENTEXT™

Migrating to SHA-2 Certificates

Frequently Asked Questions

How do I use this document?

This FAQ provides answers to some of the most frequently asked questions by our customers regarding our plans to transition from SHA-1 to SHA-2 certificates. This document will be hosted on http://www.opentext.com/campaigns/sha2.

What is SHA-2?

SHA-2 is a cryptographic hash algorithm that was first published by the U.S. National Security Agency in 2001. SHA stands for Secure Hash Algorithm. SHA hash functions are used in security applications and protocols such as TLS and SSL, and in conjunction with public-key algorithms for both encryption and digital signatures.

Why is OpenText transitioning from SHA-1 to SHA-2 certificates?

With recent advances in cryptographic attacks, network security experts have warned that using SHA-1 certificates could allow an attacker to spoof content, perform phishing attacks, or perform "man-in-the-middle" attacks. Although this potential vulnerability is not with the OpenText™ Trading Grid™, OpenText Information Exchange, OpenText EasyLink GMS or OpenText EasyLink ICC.Net, we are moving to SHA-2 certificates as part of our ongoing effort to help maintain the highest levels of data integrity and security for our customers.

The encryption hash used in SHA-2 is significantly stronger and not subject to the same vulnerabilities as SHA-1.

To find out if your internal systems support SHA-2, please visit https://www.digicert.com/sha-2-compatibility.htm

What is OpenText doing to move to SHA-2?

OpenText will start renewing all certificates as SHA-2 when the current certificate expires. We plan to completely transition from SHA-1 to SHA-2 certificates by **January 1, 2017**, the date by which Microsoft® has announced they will cease their support for SHA-1 certificates. SHA-2 certificates will be issued by our current certificate authority Comodo.

Note: *We reserve the right to upgrade pre-production environment certificates before they expire to allow customers time to test with their trading partners.*

How does this affect me?

If you or your trading partner uses FTPS, AS2, RosettaNet, OFTP, MQ, AS3 or another protocol to establish a digitally signed or encrypted message exchange connection with the Trading Grid™, Information Exchange, EasyLink GMS, or EasyLink ICC.Net, OpenText recommends that you begin preparing to replace your SHA-1 certificates with SHA-2 certificates to enhance security protections.

What do I need to do?

To prepare for this change and help ensure a smooth certificate renewal process:

1. Check with your service or software provider to ensure that your communications software supports SHA-2 certificates issued by Comodo.
    a. If yes, you will be ready to coordinate your transition to the more secure SHA-2 certificate when your current OpenText public key certificate expires.
    b. If no, and your current communications software provider is unable to assist you, please contact your OpenText Customer Manager to discuss the options available to you.
2. Contact your trading partners and have them perform the same verification with their communications software providers to ensure that their communications software supports SHA-2 certificates issued by Comodo, our current certificate authority vendor.

Will the certificate renewal process change?

There will be no change to the certificate renewal processes. However, OpenText may renew certificates as SHA-2 prior to their expiration date to ensure compliance before the January 1, 2017 deadline.

What if my current OpenText public key certificate expires after December 31, 2016?

OpenText will proactively contact customers with current OpenText public key SHA-1 certificates to help them transition to SHA-2 certificates before the January 1, 2017 deadline.

What services are affected by this change?

This change affects all SSL browser certificates and certain communications protocols. If you connect to OpenText using a modern web browser, you will not be affected by the certificate upgrade.

Note: *this does not currently affect SSH, PGP, or GPG encryption keys.*

What protocols are affected by this change?

The following protocols are affected by the transition to SHA-2 certificates:

- AS2
- AS3
- HTTPs
- SSL-FTP (FTPs)
- RosettaNet
- MQ
- Sterling/IBM – Connect:Direct Secure Plus

Which SHA-2 hash functions does OpenText currently support?

OpenText currently supports certificates signed by the following versions of SHA-2:

- SHA256
- SHA384
- SHA512

Moving forward, OpenText plans to support additional types of SHA-2 certificates. Further details will be communicated as they become available.

My communications software cannot support SHA-2 certificates. What do I do?

Although OpenText recommends transitioning to SHA-2 certificates as the most effective way to help maintain data integrity and security, we understand that not all customers can support SHA-2 certificates.

If your software does not support SHA-2or self-signed certificates, the Certificates Exchange Team will work with you to provide an alternative for up to one year. After December 31, 2015, OpenText will no longer provide alternative certificate issuance options. Beginning in 2016, the Certificates Exchange team will disable all SHA-1 certificate issuance options requiring customers to move to a SHA-2 or self-signed certificate. If you are still unable to support SHA-2 certificates at that time, the Certificate Exchange team will work with you to implement a self-signed SHA-1 certificate.

Certificates Exchange Team

Email: CertificateExchange@opentext.com
Telephone: 1-800-334-2255 x2378 (CERT)

What is Comodo?

Comodo is OpenText's primary certificate authority. Certificate authorities are organizations that issue and manage digital certificates. For more information, visit Comodo's website at www.comodo.com.

Why did OpenText switch to Comodo?

OpenText chose Comodo because it offers a complete range of digital certificates with the strongest encryption available, and the technical capability and flexibility to meet enterprise needs. As a WebTrust Certificate Authority (CA), Comodo meets the highest standards of confidentiality, system reliability and pertinent business practices through qualified independent audits.

Could the switch to Comodo have an impact on my services?

Switching to a Comodo issued certificate should have little impact on newer file exchange products. As Comodo is a relatively new Certificate Authority, customers with older file exchange products (>10 years) may experience issues loading the root and intermediate certificates into their certificate store. For more information, visit Comodo's website at www.comodo.com.

***Note**: Customers with older file exchange products or self-developed software should load all chained certificates (.p7b). If you use the .cer versions, please ensure all three Comodo certificates are loaded into your certificate store.*

Who should I contact for further information?

For more information, OpenText Trading Grid and Information Exchange customers can contact Cloud Support Services.

OpenText EasyLink GMS and ICC.Net customers can contact OpenText EasyLink Customer Support.

For Sterling Connect:Direct users only

How do I know if my Sterling Connect:Direct software version is SHA-2 compliant?

For more information on SHA-2 support for Sterling Connect:Direct, please refer to the SHA-2 Support guide on IBM's website. You can access the guide by visiting the link below:

ftp://ftp.software.ibm.com/software/commerce/doc/mft/cdcommon/secplus_SHA2SupportForCD_Book.pdf

Refer to ***Table 2. SHA-2 Compatible Software*** to see if your version of Connect:Direct supports SHA-2. If your version is not SHA-2 compatible, you have a number of options available to you. These include:

1. Upgrading your Connect:Direct software to a version that supports SHA-2.
2. Contacting your OpenText representative to install/configure another protocol for data transmission.

Note: If you are only sending **inbound** files through OpenText, you may not experience any issues. However, unless your system can support SHA-2 certificates, OpenText will not be able to send you any data files.

What are the standard pre-requisites to connect to OpenText using Connect:Direct?

Standard pre-requisites include:

- OpenText only installs / adds customer Root Certificate Authorities and/or Intermediate certificates into our Trusted Store
- Certificates sent to OpenText should not be self-signed. OpenText will not accept a self-signed certificate
- Client Authentication should be turned off
- OpenText prefers that certificates be in Base64 encoded format
- All cipher-suites should be added to the Secure+ setup

- OpenText is configured for TLSv1

What certificates will I need to install on my Connect:Direct system to enable a connection with OpenText?

Customers will need to install the following new certificates as separate files:

- Public Certificate (should contain the certificates in the chain)
- Intermediate Certificate (should contain the chain with just the Root CA)
- Root CA Certificate

What should I do with the new certificates?

Customers should install/add the applicable certificates into their Secure+ setup for OpenText's Connect:Direct node or consult with their internal technical contact and/or IBM Support.

Do I remove your previous certificates?

The requirement to remove previous certificates depends on your particular Connect:Direct Secure+ setup. Please consult with your internal technical contact and/or IBM Support.

Are any other Secure+ settings required to support SHA-2 certificates?

No. However, customers can make the following changes at their option.

- Add all cipher suites to the Secure+ setup
- Remove weak or broken cipher suites

Do I have to test using the SHA-2 certificate?

OpenText recommends that customers test their new certificates to ensure they work as expected. If any issues are encountered, customers should open a product service request with Cloud Support Services.

What if my certificate expires?

An expired certificate normally means that the Public certificate has expired but not the Intermediate or Root CA. In many instances, you do not have to do anything with the actual certificates because the Intermediate and/or Root CA have not changed. If the Intermediate and/or the Root CA are new, please have them added to the Trusted Store.

About OpenText

OpenText enables the digital world by simplifying, transforming, and accelerating enterprise information needs, on premises or in the cloud. For more information about OpenText Cloud Services (NASDAQ: OTEX, TSX: OTC) visit www.gxs.com.

Connect with us:

- OpenText CEO Mark Barrenechea's blog
- Twitter | LinkedIn | Facebook

www.gxs.com/support | www.easylink.com/support

NORTH AMERICA +800 334 2255 • UNITED STATES +1 301 251 65100

OTHER LOCATIONS http://techsupport.gxs.com/regional-directories