GO ANYWHERE®
Managed File Transfer

GUIDE *(Cybersecurity)*

What's New in PCI Data Security Standard 3.2

Implications for Managed File Transfer Solutions

WHAT'S NEW IN PCI DATA SECURITY STANDARD 3.2

Implications for Managed File Transfer Solutions

If you work for any organization that processes credit or debit cards, you've already faced the pressure to achieve and maintain PCI DSS compliance. The Payment Card Industry Data Security Standard (PCI DSS) is a proprietary information security standard for organizations that process credit or debit cards.

The standard is a moving target since it is frequently updated to address new security threats or clarify issues that have been problems in past versions. Version 3.2 of PCI DSS was announced in April 2016 and the process of shifting from version 3.1 to version 3.2 is currently underway. Although PCI DSS 3.1 expired in October 2016, all updated requirements will be considered best practices until February 1, 2018, when they will become mandatory. There is one exception: the deadline for migrating from SSL and early TLS was pushed out to June 2018.

Being up-to-date with current compliance standards ensures that you avoid hefty fines and protects you against a potentially costly data breach. Here's what you need to know to be ready for PCI DSS 3.2.

Why is PCI DSS Being Updated?

Cybersecurity is an ever changing field that expands to cover new technology and new threats all the time. The PCI Security Standards Council updates PCI DSS regulations in order to address new concerns and provide greater clarity regarding existing requirements.

In this case, the surprise for some was that PCI DSS only jumped to version 3.2, instead of version 4. This is because PCI DSS is now seen as a mature standard that doesn't require the significant updates that have been seen in the past. Future updates to PCI DSS are likely to be incremental as well.

Who Has to Comply with the New Standard?

Anyone processing cardholder data should be paying attention to PCI DSS compliance. However, not every PCI DSS requirement applies to every organization. While some of the changes in version 3.2 apply to all entities that fall under PCI DSS, several updates are aimed specifically at service providers.

PCI DSS 3.2 Compliance Deadline: February 1, 2018.

Appendix A3—the DESV—applies only to entities designated by payment brands or acquirers as needing additional assessment.

What is Different in PCI DSS Version 3.2?

While many requirements were slightly reworded for the sake of clarity or to take changing industry terminology into account, there are five main updates you need to get ready for. The three that apply to everyone are multifactor authentication, SSL and TLS migration, and PAN storage. If you are a service provider or fall under the DESV (which stands for Designated Entities Supplemental Validation), you will have additional considerations.

Multifactor Authentication

Protecting administrative access to the cardholder data environment (CDE) is imperative. Regardless of the method used to gain access to a network, the goal of an intruder is typically to find a device to which they can gain administrative rights. Once they have that, they can move throughout the network, gaining access on additional machines until they reach the cardholder data. Multifactor authentication provides an added layer of protection at critical points.

Requirement 8.3 in the previous version of PCI DSS stated that organizations need to incorporate two-factor authentication for remote network access originating from outside the network. In version 3.2, the term "two-factor authentication" is changed to "multi-factor authentication" to reflect the possibility of having more than two forms of authentication, and the requirement is expanded to include all individual non-console administrative access as well as all remote access to the CDE. With this change, anyone who allows any kind of non-console access will need

multi-factor authentication, regardless of whether that access is happening remotely, from within the organization's own network, or from the CDE itself.

SSL and Early TLS Migration

The Secure Sockets Layer (SSL) first appeared in the 1990s and grew to be a widely accepted security standard. However, SSL is now considered to have several vulnerabilities. In 1999, version 3.1 of SSL was released as Transport Layer Security (TLS) 1.0. While TLS improved on the security of SSL, TLS version 1.0—and in some cases 1.1—is no longer considered strong. Version 3.2 of PCI DSS requires organizations to work toward upgrading to a strong cryptographic protocol, meaning at least TLS 1.1, although TLS 1.2 is strongly recommended.

This applies to a few PCI DSS requirements that require strong cryptography or additional security features: requirements 2.2.3, 2.3, and 4.1. PCI DSS version 3.2 started requiring that all service providers deploy a secure service offering in June 2016. For other entities, SSL and early TLS must not be used for any new implementations. Organizations have until June 30, 2018 to implement newer TLS versions to existing implementations. Prior to that date, existing implementations using SSL or early TLS must have a formal Risk Mitigation and Migration Plan in place.

PCI DSS 3.2 requirement updates regarding Multi-factor Authentication, SSL & TLS Migration and PAN Storage APPLY TO EVERYONE.

PCI DSS Compliance for Service Providers

Service providers play a critical role in keeping card-holder data protected for their customers, and weaknesses in their security practices have been a common factor in breaches. According to a Ponemon Institute study, nearly half of risk professionals say their organization experienced a data breach caused by one of their vendors. 73 percent see the number of cybersecurity incidents involving vendors increasing, and 65 percent find it difficult to manage security incidents involving vendors.

PCI DSS 3.2 introduces several new security requirements for service providers, mostly to hold the providers more accountable for the security of their customers. Service providers will now have to detect and notify customers of failing critical security control systems. Third-party penetration testing is required every six months, rather than annually as was required by the previous version of PCI DSS. Quarterly reviews are required of employees and their respective access to the CDE. Finally, service providers will have to provide documentation of their encryption architecture.

Designated Entities Supplemental Validation (DESV)

The DESV, or Appendix A3 of PCI DSS version 3.2, applies only to entities designated by a payment brand or acquirer as requiring additional validation. For example, this could be because they are storing and transmitting an especially large volume of cardholder data, or because they have had issues with breaches in the past. However, it is recommended that all organizations follow the outlined procedures.

The DESV aims to make PCI DSS compliance an ongoing practice, rather than a hurdle which is cleared and then forgotten. Verizon's most recent study of PCI compliance found that only 29 percent of companies are still compliant a year after validation. DESV organizations must implement a PCI DSS compliance program and validate that PCI DSS best practices are incorporated into business-as-usual activities, among other requirements.

How Does PCI DSS 3.2 Affect Managed File Transfer?

Almost every organization deals with file transfers, and if you are required to comply with PCI DSS, you'll want to make sure you are using a managed file transfer solution that enables you to achieve compliance with the new version of the regulation.

What does that mean?

First of all, your managed file transfer (MFT) software needs to support TLS 1.1 and 1.2 to ensure compliance and up-to-date encryption standards. Secondly, the solution should support role-based security with multi-factor authentication. PCI DSS requires multi-factor authentication at either the network level or system level.

The DESV may or may not apply to you, but either way you should be considering how you will maintain PCI DSS compliance year-round without adding too much time and effort to the IT workload. Robust MFT solutions streamline the work by providing the security features and detailed reports that auditors want to see. Some MFT software can even help you easily check if your file transfers are PCI DSS compliant.

If you haven't implemented a managed file transfer solution yet, with the latest PCI DSS version 3.2, now is the perfect time. MFT will help you comply not only with this PCI DSS version but future updates as well, as a good file transfer solution will continue to introduce security features to keep pace with current threats.

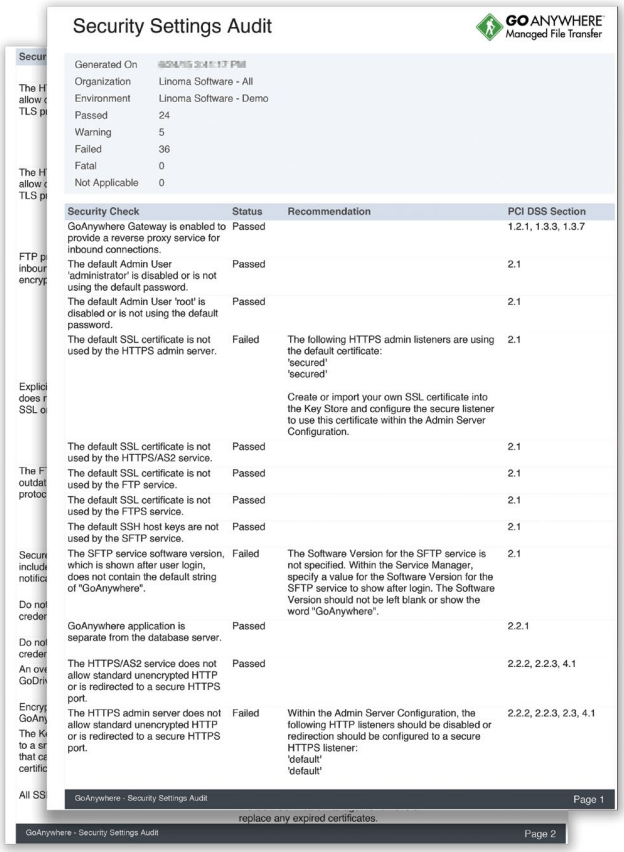
Bonus: For GoAnywhere® MFT Users

Good news for GoAnywhere Managed File Transfer users! GoAnywhere MFT provides tools to help you keep your data transfers compliant with PCI DSS. GoAnywhere supports TLS 1.1 and 1.2 and can integrate with LDAP and external RSA multi-factor authentication.

Furthermore, GoAnywhere MFT's Advanced Reporting Module can generate a Security Settings Audit Report to easily let you know if the security settings on your GoAnywhere installation are fully aligned with PCI DSS requirements. In addition to the status check, the report provides recommended actions and lets you know which section of PCI DSS the setting applies to.

The PCI DSS standard will continue to evolve, but by implementing robust solutions, forward-thinking IT shops can meet current requirements while laying a strong foundation for future security enhancements.

JUNE 30, 2018
is the deadline to migrate existing TLS implementations to new TLS versions.



Security Settings Audit

GO ANYWHERE Managed File Transfer

Generated On	[redacted]
Organization	Linoma Software - All
Environment	Linoma Software - Demo
Passed	24
Warning	5
Failed	36
Fatal	0
Not Applicable	0

Security Check	Status	Recommendation	PCI DSS Section
GoAnywhere Gateway is enabled to provide a reverse proxy service for inbound connections.	Passed		1.2.1, 1.3.3, 1.3.7
The default Admin User 'administrator' is disabled or is not using the default password.	Passed		2.1
The default Admin User 'root' is disabled or is not using the default password.	Passed		2.1
The default SSL certificate is not used by the HTTPS admin server.	Failed	The following HTTPS admin listeners are using the default certificate: 'secured' 'secured' Create or import your own SSL certificate into the Key Store and configure the secure listener to use this certificate within the Admin Server Configuration.	2.1
The default SSL certificate is not used by the HTTPS/AS2 service.	Passed		2.1
The default SSL certificate is not used by the FTP service.	Passed		2.1
The default SSL certificate is not used by the FTPS service.	Passed		2.1
The default SSH host keys are not used by the SFTP service.	Passed		2.1
The SFTP service software version, which is shown after user login, does not contain the default string of "GoAnywhere".	Failed	The Software Version for the SFTP service is not specified. Within the Service Manager, specify a value for the Software Version for the SFTP service to show after login. The Software Version should not be left blank or show the word "GoAnywhere".	2.1
GoAnywhere application is separate from the database server.	Passed		2.2.1
The HTTPS/AS2 service does not allow standard unencrypted HTTP or is redirected to a secure HTTPS port.	Passed		2.2.2, 2.2.3, 4.1
The HTTPS admin server does not allow standard unencrypted HTTP or is redirected to a secure HTTPS port.	Failed	Within the Admin Server Configuration, the following HTTP listeners should be disabled or redirection should be configured to a secure HTTPS listener: 'default' 'default'	2.2.2, 2.2.3, 2.3, 4.1

GoAnywhere - Security Settings Audit Page 1

replace any expired certificates.

GoAnywhere - Security Settings Audit Page 2

Get started with PCI compliance today.

Download your free 30-day GoAnywhere trial by visiting www.goanywhere.com/trial.
You can also contact us by emailing goanywhere.sales@helpsystems.com.

About GoAnywhere

GoAnywhere® Managed File Transfer is an enterprise-ready managed file transfer solution which streamlines and encrypts the exchange of data between your systems, employees, customers and trading partners. It provides a single point of control with extensive security settings, detailed audit trails and reports.

GoAnywhere® Gateway is both an enhanced reverse proxy and forward proxy that provides an additional layer of security when exchanging data with your trading partners by closing inbound ports into your private network and keeping sensitive data out of your DMZ.

Learn more about the GoAnywhere Managed File Transfer solution at www.GoAnywhere.com.

HelpSystems
103 S 14th St
Ashland, Nebraska 68003
(402) 944.4242
(800) 949.4696
goanywhere.sales@helpsystems.com
www.GoAnywhere.com

helpsystems

www.helpsystems.com

About HelpSystems

Organizations around the world rely on HelpSystems to make IT lives easier and keep business running smoothly. Our software and services monitor and automate processes, encrypt and secure data, and provide easy access to the information people need.