Security Settings Audit

GO ANYWHERE® Managed File Transfer

Generated On	Month/Date/Year Time AM/PM
Organization	Sample
Environment	Sample
Passed	50
Warning	3
Failed	30
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, 1.3.2, 1.3.6, 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 certificate is not used by the HTTPS admin server.	Passed		2.1
The default certificate is not used by the HTTPS/AS2/AS4 service.	Passed		2.1
The default certificate is not used by the FTP service.	Passed		2.1
The default 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".	Passed		2.1
GoAnywhere application is separate from the database server.	Passed		2.2.1
The HTTPS/AS2/AS4 service does not allow standard unencrypted HTTP or is redirected to a secure HTTPS port.	Warning	Within the Service Manager, verify that the following HTTP listeners are redirecting to secure HTTPS listeners: 'plain' 'plain'	2.2.2, 2.2.3, 4.1

Security Check	Status	Recommendation	PCI DSS Section
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
The control channel between GoAnywhere MFT and GoAnywhere Gateway is encrypted using SSL/TLS.	Failed	Enable SSL in the Control Channel Security section of the Gateway Configuration screen in GoAnywhere MFT. You must also enable SSL in the Gateway software installation.	2.2.3
A Shared Secret is used to establish trust between GoAnywhere MFT and GoAnywhere Gateway.	Failed	Specify a Shared Secret in the Gateway Configuration within GoAnywhere MFT. This same Shared Secret must also be specified in the Gateway software installation.	2.2.3
The HTTPS admin server does not allow outdated versions of SSL or TLS protocols.	Failed	Within the Admin Server Configuration, the following HTTPS admin listeners should be configured to only allow SSL protocol versions TLSv1.1 and TLSv1.2: 'secured' 'secured'	2.2.3, 2.3, 4.1
The HTTPS/AS2/AS4 service does not allow outdated versions of SSL or TLS protocols.	Passed		2.2.3, 4.1
FTP protocol is not allowed for inbound connections unless it is encrypted.	Failed	Standard FTP is enabled and Explicit SSL encryption is not specified for the following FTP listeners: 'default' 'default' Within the Service Manager, the FTP server should be disabled or Explicit SSL should be enforced by enabling the 'Force Encrypted Authentication' and 'Force Encrypted Data Channels' settings for the FTP Server.	2.2.2, 2.2.3, 4.1
Explicit SSL on the FTP service does not allow outdated versions of SSL or TLS protocols.	Failed	Within the Service Manager, the following FTP service listeners should be configured to only allow SSL protocol versions TLSv1.1 and TLSv1.2: 'default' 'default'	2.2.3, 4.1
The FTPS service does not allow outdated versions of SSL or TLS protocols.	Passed		2.2.3, 4.1
Secure Mail passwords are not included in the primary email notification.	Failed	In the Secure Mail Settings, disable the ability to include passwords in email notifications or require that those passwords are sent in a	2.2.4

Security Check	Status	Recommendation	PCI DSS Section
		separate email.	
Do not allow browsers to save login credentials for Admin Users.	Passed		2.2.4
Do not allow browsers to save login credentials for Web Users.	Passed		2.2.4
Administrators with the Resource Manager role are not allowed to view passwords on Resources.	Failed	Disable the Allow Viewing of Resource Passwords setting in the Admin Security Settings.	2.2.4
An overall disk quota is specified for GoDrive.	Passed		3.1
Encrypted folders are configured in GoAnywhere.	Passed		3.4
The Key Manager role is restricted to a small number of Admin Users that can create/manage keys and certificates.	Warning	More than 2 Admin Users have authority to the Key Manager role. It is recommended to restrict this role to essential Admin Users.	3.5.2, 7.1
All certificates are current.	Failed	One or more certificates are expired. Use the Certificate Manager to remove or replace any expired certificates.	3.6.5
All PGP keys are current.	Failed	One or more PGP keys are expired. Use the PGP Key Manager to remove or replace any expired keys.	3.6.5
Only FIPS 140-2 validated encryption ciphers are used for SSL and SSH channels, which is applicable to FTPS, HTTPS, AS2, AS4, SFTP and SCP protocols.	Warning	Enable the FIPS 140-2 Compliance mode to use only validated and strong cipher algorithms for SSL and SSH channels.	4.1
The HTTPS admin server uses only the strong ciphers of AES and TDES (3DES).	Passed		4.1
The HTTPS/AS2/AS4 service uses only the strong ciphers of AES and TDES (3DES).	Passed		4.1
Explicit SSL on the FTP service uses only the strong ciphers of AES and TDES (3DES).	Passed		4.1
The FTPS service uses only the strong ciphers of AES and TDES (3DES).	Passed		4.1
The SFTP service uses only the strong ciphers of AES and TDES (3DES).	Passed		4.1
The HTTPS admin server does not use outdated Mac Algorithms.	Passed		4.1
The HTTPS/AS2/AS4 service does not use outdated Mac Algorithms.	Passed		4.1
Explicit SSL on the FTP service does not use outdated Mac Algorithms.	Passed		4.1
The FTPS service does not use outdated Mac Algorithms.	Passed		4.1

Security Check	Status	Recommendation	PCI DSS Section
The HTTPS admin server does not use weak Diffie Hellman key exchange algorithms.	Passed		4.1
The HTTPS/AS2/AS4 service does not use weak Diffie Hellman key exchange algorithms.	Passed		4.1
Explicit SSL on the FTP service does not use weak Diffie Hellman key exchange algorithms.	Passed		4.1
The FTPS service does not use weak Diffie Hellman key exchange algorithms.	Passed		4.1
The SFTP service does not use outdated Mac Algorithms.	Passed		4.1
GoAnywhere product software was updated within the last 6 months.	Passed		6.2
Java Runtime Environment (JRE) for the GoAnywhere product is at version 1.8 or higher.	Passed		6.2
HTTPS Web Client does not allow embedding within an IFrame.	Failed	In the Service Manager, configure the HTTPS Web Client preferences to disable 'Allow Embedding within an IFrame'.	6.5.7, 6.6
HTTPS Web Client does not allow the Session ID to be stored in the URL.	Passed		6.5.10, 6.6
Brute Force Attacks are monitored and blocked with IP auto-blacklisting.	Passed		6.6
Denial-of-Service (DoS) Attacks are monitored and blocked with IP auto-blacklisting.	Passed		6.6
IP Filtering is enabled to be performed in the GoAnywhere Gateway.	Passed		6.6
Restrict the role of Security Officer (the highest level of authority) to a small number of Admin Users.	Failed	More than 2 Admin Users have authority to the Security Officer role, which can be used to access all administrator features in GoAnywhere. It is recommended to restrict this role to essential Admin Users.	7.1
All Admin User accounts have been active within the last 90 days.	Failed	59 Admin User accounts are enabled and have not logged in within the last 90 days. These accounts should be disabled or deleted.	8.1.4
All Web User accounts have been active within the last 90 days.	Failed	38 Web User accounts are enabled and have not logged in within the last 90 days. These accounts should be disabled or deleted.	8.1.4
Web Users are automatically disabled when no activity for 90 days.	Failed	The following Web Users should be configured to have a 'Disable Account When No Activity' setting of 90 days or less: Sample Sample	8.1.4

Security Check	Status	Recommendation	PCI DSS Section
		... and 21 other web users	
Web User accounts are disabled after no more than 6 login failures.	Passed		8.1.6, 8.1.7
The HTTPS admin server requires a user to re-authenticate if the session has been idle for more than 15 minutes.	Failed	Change the 'Session Timeout' to 900 seconds or less in the Admin Security Settings.	8.1.8
The HTTPS/AS2/AS4 service requires a user to re-authenticate if the session has been idle for more than 15 minutes.	Passed		8.1.8
The FTP service requires a user to re-authenticate if the session has been idle for more than 15 minutes.	Passed		8.1.8
The FTPS service requires a user to re-authenticate if the session has been idle for more than 15 minutes.	Passed		8.1.8
The SFTP service requires a user to re-authenticate if the session has been idle for more than 15 minutes.	Passed		8.1.8
The default AS2 service settings require trading partner authentication or signatures for inbound AS2 messages.	Passed		8.2
All AS2 Web User accounts require authentication or signatures for inbound AS2 messages.	Passed		8.2
Minimum password length for Admin Users is at least 7 characters.	Passed		8.2.3
Passwords for Admin Users should contain both numeric and alphabetic characters.	Failed	Enforce and configure the Password Policy in the Admin Security Settings to require at least one Letter and one Digit.	8.2.3
Minimum password length for Web Users is at least 7 characters.	Passed		8.2.3
Passwords for Web Users should contain both numeric and alphabetic characters.	Passed		8.2.3
For Web Users that authenticate against the GoAnywhere login method, the maximum password age is 90 days or less.	Passed		8.2.4
For Web Users that authenticate against the GoAnywhere login method, the password expiration interval is 90 days or less.	Failed	The following Web Users should be configured to have a 'Password Expiration Interval' of 90 days or less: SampleUser1 SampleUser2	8.2.4

Security Check	Status	Recommendation	PCI DSS Section
		... and 22 other web users	
For Admin Users that authenticate against the GoAnywhere login method, the maximum password age is 90 days or less.	Failed	Enable and configure the Password Policy in the Admin Security Settings to require the Maximum Password Age of 90 days or less.	8.2.4
For Web Users that authenticate against the GoAnywhere login method, they are not allowed to reuse their last 4 passwords.	Passed		8.2.5
Admin Users that authenticate against the GoAnywhere login method are not allowed to reuse their last 4 passwords.	Failed	Enable and configure the Password Policy in the Admin Security Settings to enforce password history and disallow the reuse of the last 4 passwords.	8.2.5
For Web Users that authenticate against the GoAnywhere login method, their password must be changed after the first login.	Failed	The following Web User Templates should be configured to force password change at next login: 'Sample User' 'Sample User 2' 'Sample User 3' 'Sample User 4'	8.2.6
All Admin Users are utilizing multi-factor authentication.	Failed	The 'root' and/or 'administrator' users are currently enabled. These are default accounts that only use the internal GoAnywhere login method and cannot be configured for multi-factor authentication.	8.3.1
All Web Users are utilizing multi-factor authentication for 'HTTPS'.	Failed	The following Web Users should be configured to use multi-factor authentication for 'HTTPS': Sample User Sample User 2 Sample User 3 Sample User 4 ... and 86 other web users	8.3.2
All Web Users are utilizing multi-factor authentication for 'AS2'.	Failed	The following Web Users should be configured to use multi-factor authentication for 'AS2': Sample User Sample User 2 Sample User 3 Sample User 4 ... and 18 other web users	8.3.2
All Web Users are utilizing multi-factor	Failed	The following Web Users should be configured to use multi-factor	8.3.2

Security Check	Status	Recommendation	PCI DSS Section
authentication for 'AS4'.		authentication for 'AS4': Sample User 1 Sample User 2 Sample User 3 Sample User 4 ... and 1 other web user	
All Web Users are utilizing multi-factor authentication for 'FTPES'.	Failed	The following Web Users should be configured to use multi-factor authentication for 'FTPES': Sample User 1 Sample User 2 Sample User 3 Sample User 4 ... and 75 other web users	8.3.2
All Web Users are utilizing multi-factor authentication for 'FTPS'.	Failed	The following Web Users should be configured to use multi-factor authentication for 'FTPS': Sample User 1 Sample User 2 Sample User 3 Sample User 4 ... and 72 other web users	8.3.2
All Web Users are utilizing multi-factor authentication for 'SFTP'.	Failed	The following Web Users should be configured to use multi-factor authentication for 'SFTP': Sample User 1 Sample User 2 Sample User 3 Sample User 4 ... and 76 other web users	8.3.2
All Web Users are utilizing multi-factor authentication for 'GoFast'.	Failed	The following Web Users should be configured to use multi-factor authentication for 'GoFast': Sample User 1 Sample User 2 Sample User 3 Sample User 4 ... and 12 other web users	8.3.2
Anonymous users are not allowed to access services.	Failed	Configure the Web User Settings to disable the Anonymous Web User.	8.5
At least 3 months of Audit Trails are immediately	Passed		10.7

Security Check	Status	Recommendation	PCI DSS Section
available for analysis.			
Audit Trails are archived to disk if they are purged within 1 year.	Passed		10.7