Security Settings Audit

FORTRA GoAnywhere

Generated On	2025-12-30 10:04:22
Organization	AtriCure
Environment	ATC-GoAnywhere
Passed	46
Warning	15
Failed	22
Fatal	1
Not Applicable	18

Security Check	Status	Recommendation	PCI DSS Section
GoAnywhere Gateway is enabled to provide a reverse proxy service for inbound connections.	Passed		1.3.1, 1.3.2, 1.4.1, 1.4.2, 1.4.4, 1.4.5
The default Admin User 'administrator' is disabled or is not using the default password.	Passed		2.2.2
The default Admin User 'root' is disabled or is not using the default password.	Passed		2.2.2
GoAnywhere application is separate from the database server.	Passed		2.2.3
The HTTPS admin server does not allow standard unencrypted HTTP or is redirected to a secure HTTPS port.	Warning	Within the Admin Server Configuration, verify that the following HTTP listeners are redirecting to secure HTTPS listeners: 'default'	2.2.4, 2.2.5, 2.2.7, 4.2.1
The HTTPS/AS2/AS4 service does not allow standard unencrypted HTTP or is redirected to a secure HTTPS port.	Passed		2.2.4, 2.2.5, 4.2.1
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' 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.	2.2.4, 2.2.5, 4.2.1
A Shared Secret is used to establish trust between GoAnywhere MFT and GoAnywhere Gateway.	Passed		2.2.5
The HTTPS admin server does not allow outdated versions of SSL or TLS protocols.	Passed		2.2.5, 2.2.7, 4.2.1
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.	2.2.5, 4.2.1
The HTTPS/AS2/AS4 service does not allow outdated versions of SSL or TLS protocols.	Passed		2.2.5, 4.2.1

Security Check	Status	Recommendation	PCI DSS Section
Explicit SSL on the FTP service does not allow outdated versions of SSL or TLS protocols.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 TLSv1.2 and TLSv1.3: 'default' This can be configured under global Security Settings for all TLS services. Alternatively, you can configure enabled TLS protocols under each respective service. Please note, a restart of the application is required to apply changes made in the Security Settings page. If changes are made directly to the service, only a service restart is required.	2.2.5, 4.2.1
The FTPS service does not allow outdated versions of SSL or TLS protocols.	Passed		2.2.5, 4.2.1
The GoFast service does not allow outdated versions of SSL or TLS protocols.	Not Applicable		2.2.5, 4.2.1
The PeSIT service does not allow outdated versions of SSL or TLS protocols.	Not Applicable		2.2.5, 4.2.1
The Agent service does not allow outdated versions of SSL or TLS protocols.	Passed		2.2.5, 4.2.1
The default certificate is not used by the HTTPS admin server.	Passed		2.2.7, 4.2.1
An overall disk quota is specified for GoDrive.	Failed	Enable 'Limit Disk Space' and then specify 'Maximum Disk Space' within GoDrive Settings.	3.2
Encrypted folders are configured in GoAnywhere.	Warning	It is recommended to use the Encrypted Folders function in GoAnywhere for storing sensitive files.	3.5.1
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.	3.6.1.3, 7.2.2
All certificates are current.	Passed		3.7.5
All PGP keys are current.	Passed		3.7.5
Only FIPS 140-2 validated encryption ciphers are used for SSL and SSH channels, which is applicable to all SSL and SSH based protocols.	Warning	Enable the FIPS 140-2 Compliance mode to use only validated and strong cipher algorithms for SSL and SSH channels.	4.2.1
The default certificate is not used by the HTTPS/AS2/AS4 service.	Passed		4.2.1
The default certificate is not used by the FTP service.	Failed	The following FTP service listeners are using the default certificate: 'default' Create or import your own certificate into the Key Store and configure the FTP service to use this certificate within the Service Manager.	4.2.1
The default certificate is not used by the FTPS service.	Fatal		4.2.1
The default certificate is not used by the GoFast service.	Not Applicable		4.2.1
The default certificate is not used by the PeSIT service.	Not Applicable		4.2.1

Security Check	Status	Recommendation	PCI DSS Section
The default SSH host keys are not used by the SFTP service.	Passed		4.2.1
The HTTPS admin server does not use weak cipher algorithms.	Warning	The following listeners are using cipher suites that rely on the CHACHA algorithm: 'secured' Consider disabling cipher suites that use the CHACHA algorithm on your listener. This can be configured under Security Settings for all TLS services. Alternatively, this can be configured in the Admin Server Configuration. Please note, a restart of the application is required to apply changes made in the Security Settings page. If changes are made directly to the service, only a service restart is required.	4.2.1
The HTTPS/AS2/AS4 service does not use weak cipher algorithms.	Warning	The following listeners are using cipher suites that rely on the CHACHA algorithm: 'default' Consider disabling cipher suites that use the CHACHA algorithm on your listener. This can be configured under Security Settings for all TLS services. Alternatively, you can select cipher suites individually under each respective service. Please note, a restart of the application is required to apply changes made in the Security Settings page. If changes are made directly to the service, only a service restart is required.	4.2.1
Explicit SSL on the FTP service does not use weak cipher algorithms.	Warning	The following listeners are using cipher suites that rely on the CHACHA algorithm: 'default' Consider disabling cipher suites that use the CHACHA algorithm on your listener. This can be configured under Security Settings for all TLS services. Alternatively, you can select cipher suites individually under each respective service. Please note, a restart of the application is required to apply changes made in the Security Settings page. If changes are made directly to the service, only a service restart is required.	4.2.1
The FTPS service does not use weak cipher algorithms.	Warning	The following listeners are using cipher suites that rely on the CHACHA algorithm: 'default' Consider disabling cipher suites that use the CHACHA algorithm on your listener. This can be configured under Security Settings for all TLS services. Alternatively, you can select cipher suites individually under each respective service. Please note, a restart of the application is required to apply changes made in the Security Settings page. If changes are made directly to the service, only a service restart is required.	4.2.1
The GoFast service does not use weak cipher algorithms.	Not Applicable		4.2.1
The PeSIT service does not use weak cipher algorithms.	Not Applicable		4.2.1
The Agent service does not use weak cipher algorithms.	Warning	The following listeners are using cipher suites that rely on the CHACHA algorithm: 'SSL' Consider disabling cipher suites that use the	4.2.1

Security Check	Status	Recommendation	PCI DSS Section
		CHACHA algorithm on your listener. This can be configured under Security Settings for all TLS services. Alternatively, you can select cipher suites individually under each respective service. Please note, a restart of the application is required to apply changes made in the Security Settings page. If changes are made directly to the service, only a service restart is required.	
The SFTP service does not use weak cipher algorithms.	Passed		4.2.1
The HTTPS admin server does not use weak MAC algorithms.	Warning	The following listeners are using cipher suites that rely on the SHA-1 MAC algorithm: 'secured' Consider disabling cipher suites that use the SHA-1 algorithm on your listener. This can be configured under Security Settings for all TLS services. Alternatively, this can be configured in the Admin Server Configuration. Please note, a restart of the application is required to apply changes made in the Security Settings page. If changes are made directly to the service, only a service restart is required.	4.2.1
The HTTPS/AS2/AS4 service does not use weak MAC algorithms.	Warning	The following listeners are using cipher suites that rely on the SHA-1 MAC algorithm: 'default' Consider disabling cipher suites that use the SHA-1 algorithm on your listener. This can be configured under Security Settings for all TLS services. Alternatively, you can select cipher suites individually under each respective service. Please note, a restart of the application is required to apply changes made in the Security Settings page. If changes are made directly to the service, only a service restart is required.	4.2.1
Explicit SSL on the FTP service does not use weak MAC algorithms.	Warning	The following listeners are using cipher suites that rely on the SHA-1 MAC algorithm: 'default' Consider disabling cipher suites that use the SHA-1 algorithm on your listener. This can be configured under Security Settings for all TLS services. Alternatively, you can select cipher suites individually under each respective service. Please note, a restart of the application is required to apply changes made in the Security Settings page. If changes are made directly to the service, only a service restart is required.	4.2.1
The FTPS service does not use weak MAC algorithms.	Warning	The following listeners are using cipher suites that rely on the SHA-1 MAC algorithm: 'default' Consider disabling cipher suites that use the SHA-1 algorithm on your listener. This can be configured under Security Settings for all TLS services. Alternatively, you can select cipher suites individually under each respective service. Please note, a restart of the application is required to apply changes made in the Security Settings page. If changes are made directly to the service, only a service restart is required.	4.2.1
The GoFast service does not use	Not		4.2.1

Security Check	Status	Recommendation	PCI DSS Section
weak MAC algorithms.	Applicable		
The PeSIT service does not use weak MAC algorithms.	Not Applicable		4.2.1
The Agent service does not use weak MAC algorithms.	Warning	The following listeners are using cipher suites that rely on the SHA-1 MAC algorithm: 'SSL' Consider disabling cipher suites that use the SHA-1 algorithm on your listener. This can be configured under Security Settings for all TLS services. Alternatively, you can select cipher suites individually under each respective service. Please note, a restart of the application is required to apply changes made in the Security Settings page. If changes are made directly to the service, only a service restart is required.	4.2.1
The SFTP service does not use weak MAC algorithms.	Passed		4.2.1
The HTTPS admin server does not use weak key exchange algorithms.	Passed		4.2.1
The HTTPS/AS2/AS4 service does not use weak key exchange algorithms.	Passed		4.2.1
Explicit SSL on the FTP service does not use weak key exchange algorithms.	Failed	Configure the following FTP listeners to only select cipher suites that use ephemeral Diffie Hellman (DHE or ECDHE) key exchange algorithms: 'default' This can be configured under global Security Settings for all TLS services. Alternatively, you can select cipher suites individually under each respective service. Please note, a restart of the application is required to apply changes made in the Security Settings page. If changes are made directly to the service, only a service restart is required.	4.2.1
The FTPS service does not use weak key exchange algorithms.	Passed		4.2.1
The GoFast service does not use weak key exchange algorithms.	Not Applicable		4.2.1
The PeSIT service does not use weak key exchange algorithms.	Not Applicable		4.2.1
The Agent service does not use weak key exchange algorithms.	Passed		4.2.1
The SFTP service does not use weak key exchange algorithms.	Passed		4.2.1
The SFTP service software version, which is shown after user login, does not contain the default string of "GoAnywhere".	Passed		6.2.4
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 separate email.	6.2.4
Do not allow browsers to save login credentials for Admin Users.	Passed		6.2.4
Do not allow browsers to save login credentials for Web Users.	Passed		6.2.4

Security Check	Status	Recommendation	PCI DSS Section
Administrators with the Resource Manager role are not allowed to view passwords on Resources.	Passed		6.2.4
HTTPS Web Client does not allow embedding within an IFrame.	Passed		6.2.4
HTTPS Web Client does not allow the Session ID to be stored in the URL.	Passed		6.2.4
GoAnywhere product software was updated within the last 6 months.	Warning	No updates have been applied to the GoAnywhere product software since 2025-06-25. Contact Fortra to obtain the latest versions or security patches.	6.3.3
Brute Force Attacks are monitored and blocked with IP auto-blocking.	Passed		6.4.1
Denial-of-Service (DoS) Attacks are monitored and blocked with IP auto-blocking.	Passed		6.4.1
Attacks targeting specific or malicious user names are monitored and blocked with IP auto-blocking.	Passed		6.4.1
IP Filtering is enabled to be performed in the GoAnywhere Gateway.	Passed		6.4.1, 6.4.2
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.	7.2.2
Anonymous users are not allowed to access services.	Passed		8.2.2
All Admin User accounts have been active within the last 90 days.	Failed	4 Admin User accounts are enabled and have not logged in within the last 90 days. These accounts should be disabled or deleted.	8.2.6
All Web User accounts have been active within the last 90 days.	Failed	33 Web User accounts are enabled and have not logged in within the last 90 days. These accounts should be disabled or deleted.	8.2.6
Web Users are automatically disabled when no activity for 90 days.	Failed	Configure the Web User Settings to disable inactive Web User accounts after 90 days.	8.2.6
The HTTPS admin server requires a user to re-authenticate if the session has been idle for more than 15 minutes.	Passed		8.2.8
The HTTP/AS2/AS4 service requires a user to re-authenticate if the session has been idle for more than 15 minutes.	Failed	Change the HTTPS general preference of 'Session Timeout' to 900 seconds or less in the Service Manager.	8.2.8
The FTP service requires a user to re-authenticate if the session has been idle for more than 15 minutes.	Passed		8.2.8
The FTPS service requires a user to re-authenticate if the session has been idle for more than 15 minutes.	Passed		8.2.8
The SFTP service requires a user to re-authenticate if the session has been idle for more than 15 minutes.	Passed		8.2.8
The GoFast service requires a user to re-authenticate if the session has	Not Applicable		8.2.8

Security Check	Status	Recommendation	PCI DSS Section
been idle for more than 15 minutes.			
The PeSIT service requires a user to re-authenticate if the session has been idle for more than 15 minutes.	Not Applicable		8.2.8
The global AS2 service settings require trading partner authentication or signatures for inbound AS2 messages.	Not Applicable		8.3.1
All AS2 Web User accounts require authentication or signatures for inbound AS2 messages.	Not Applicable		8.3.1
Web User accounts are disabled after no more than 10 login failures.	Passed		8.3.4
Admin User accounts are disabled after no more than 10 login failures.	Passed		8.3.4
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: 'Invited Users' 'Service User for automated transfers'	8.3.5
Minimum password length for Admin Users is at least 12 characters.	Failed	Enforce and configure the Password Policy in the Admin Security Settings to require a 'Minimum Password Length' of 12 or more characters.	8.3.6, 8.6.3
Passwords for Admin Users should contain both numeric and alphabetic characters.	Passed		8.3.6, 8.6.3
Minimum password length for Web Users is at least 12 characters.	Passed		8.3.6, 8.6.3
Passwords for Web Users should contain both numeric and alphabetic characters.	Passed		8.3.6, 8.6.3
For Web Users that authenticate against the GoAnywhere login method, they are not allowed to reuse their last 4 passwords.	Failed	Configure the Password Policy in the Web User Settings to enforce password history and disallow the reuse of the last 4 passwords.	8.3.7, 8.6.3
Admin Users that authenticate against the GoAnywhere login method are not allowed to reuse their last 4 passwords.	Passed		8.3.7, 8.6.3
For Web Users that authenticate against the GoAnywhere login method, the maximum password age is 90 days or less.	Failed	Configure the Password Policy in the Web User Setting to require the 'Maximum Password Age' of 90 days or less.	8.3.9, 8.6.3
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: dayforce_ftp AdminWeb SVBBankTest SVBBank dayforce_telus_sftp ... and 1 other web user	8.3.9, 8.6.3
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.	8.3.9, 8.6.3

Security Check	Status	Recommendation	PCI DSS Section
All Admin Users are utilizing multi-factor authentication.	Failed	The following Admin Users should be configured to utilize multi-factor authentication: ilicensing svc_goanywhere tgallo a_jsantos a_bwarner ... and 3 other users	8.5.1
All Web Users are utilizing multi-factor authentication for 'HTTPS'.	Failed	SAML is enabled, however it is not configured to force IDP authentication. The following Web Users should be configured to use multi-factor authentication for 'HTTPS': kboreing@atricure.com mprewitt@atricure.com kmaxam@atricure.com ageiser@Atricure.com AdminWeb ... and 48 other web users	8.5.1
All Web Users are utilizing multi-factor authentication for 'AS2'.	Not Applicable		8.5.1
All Web Users are utilizing multi-factor authentication for 'AS4'.	Not Applicable		8.5.1
All Web Users are utilizing multi-factor authentication for 'FTP'.	Passed		8.5.1
All Web Users are utilizing multi-factor authentication for 'FTPS'.	Passed		8.5.1
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': dayforce_ftp SVBBank tgallo@atricure.com jsantos@atricure.com sftp-test ... and 2 other web users	8.5.1
All Web Users are utilizing multi-factor authentication for 'GoFast'.	Not Applicable		8.5.1
All Web Users are utilizing multi-factor authentication for 'PeSIT'.	Not Applicable		8.5.1
At least 3 months of Audit Trails are immediately available for analysis.	Passed		10.5.1
Audit Trails are archived to disk if they are purged within 1 year.	Failed	Within the Log Settings, configure the following Audit Logs to enable archiving or do not purge within 365 days: 'Completed Job Logs'	10.5.1