



GoAnywhere MFT Hardening Guide



Copyright Terms and Conditions

The content in this document is protected by the Copyright Laws of the United States of America and other countries worldwide. The unauthorized use and/or duplication of this material without express and written permission from HelpSystems is strictly prohibited. Excerpts and links may be used, provided that full and clear credit is given to HelpSystems with appropriate and specific direction to the original content. HelpSystems and its trademarks are properties of Help/Systems LLC and its group of companies. All other marks are property of their respective owners.

202205310354

Table of Contents

Introduction	5
Contacting Support	6
Operating System Recommendations	7
Getting Started	8
Encryption	9
Encrypted Folders	9
Master Encryption Keys	9
System	11
Security Settings	11
Global Settings	16
Admin Configuration	17
Database Configuration	18
System Alerts	19
IP Filter	21
IP Block Listing	22
Services	23
HTTPS/AS2/AS4	23
FTP	29
FTPS	33
SFTP	37
GoFast	40
Agent Service	41
PeSIT	42
GoAnywhere Gateway	43
Secure Mail Settings	44

Secure Forms Settings	47
Secure Form Configuration	48
Agent Configuration	49
Users	51
Admin Users	51
Admin User Groups	52
Admin User Templates	52
Admin Security Settings	53
Web Users	56
Web User Settings	58
Web User Self-Registration	61
Domains	62
Login Settings	63
Reporting	64
Log Settings	64
Security Settings Audit Report	65
Glossary	66

Introduction

HelpSystems strives to apply security best practices in the design, development, and testing of GoAnywhere MFT. However, securing a GoAnywhere MFT environment requires active participation from administrators, and the needs and operating procedures of your organization must be considered. Involve your security team throughout the hardening process.

This guide does not guarantee the security of your application or environment, however it is a resource to follow for best-practices when hardening your deployment of GoAnywhere MFT. It is written with the current cybersecurity landscape in mind and provides specific configuration guidelines for anyone involved in deploying GoAnywhere MFT.

Contacting Support

If you have questions about the content covered in this guide, please contact HelpSystems Support toll free at 1-800-949-4696 or +1-402-944-4242 if you are dialing outside of the USA. Email support is available at goanywhere.support@helpsystems.com during HelpSystems business hours.

You are encouraged to visit the knowledge base at <http://www.goanywheremft.com/forum/> to find answers to common questions. Please note that HelpSystems support policy and rates are subject to change.

U.S. Support Services are provided by HelpSystems during our normal business hours, which are from 7 a.m. to 6 p.m. (Central Time Zone), Monday through Friday, excluding holidays. Support for international customers is provided by HelpSystems Partners or the HelpSystems office in your region. International customers should contact your sales representative to confirm the terms and services offered by them.

Operating System Recommendations

This guide outlines the steps required for hardening GoAnywhere MFT. Before you begin:

- Keep your operating system, GoAnywhere MFT, GoAnywhere Gateway, and GoAnywhere Agents up to date. Security patches and enhancements are released regularly.
- Externalize your Java environment and keep it up to date with the latest version supported by GoAnywhere to stay ahead of security threats that target the JRE. For instructions on externalizing the JRE, see the GoAnywhere MFT Installation Guide.
- Limit access to the GoAnywhere installation location to a select few users, following the principle of least privilege. Due to the sensitive nature of the **ghttpsroot** and **adminroot** directories, HelpSystems recommends practicing caution when determining who has access to these locations.
- Create a service account for running the GoAnywhere application, following the principle of least privilege.
- Disable non-blocking entropy gathering on Linux, Unix, Solaris, and MacOS servers. Using blocking entropy gathering helps to generate more secure cryptographic keys. Note, this requires editing a startup script for MFT. To edit this script:
 1. Open the `goanywhere_catalina.sh` file for editing.
 2. Change the `JAVA_OPTS` section from `/dev/urandom` to `/dev/random`.

We recommend using Linux tools to help gathering entropy on the OS.

NOTE:

Enabling this option can cause slower startup times while the operating system gathers enough entropy to properly generate randomness for use in cryptographic functions.

Getting Started

This guide is organized by topic and mirrors the GoAnywhere MFT application. For example, the Secure Forms Settings topic can be found under the Services section, just as Secure Forms Settings can be found under Services on the application menu bar.

This guide makes regular reference to the GoAnywhere MFT Admin User Guide, and HelpSystems recommends that you have the User Guide readily available as you move through the hardening process.

While it is not absolutely necessary to use this guide in a linear fashion, it helps ensure that all elements of the application are considered and addressed.

WARNING:

Implementing the configuration settings recommended throughout this guide can result in unintended consequences, such as connectivity failures to systems that do not support the latest security standards. Consult with your security team and other involved parties to determine the ramifications of hardening your installation of GoAnywhere MFT. HelpSystems also recommends you first harden a test or non-production installation before applying these changes to a production instance. HelpSystems is not responsible for any damages caused by the usage of this guide.

Encryption

Encrypted Folders

The Encrypted Folders page allows authorized users to create and manage encrypted folders for use within GoAnywhere.

To manage encrypted folders:

1. Log in as an Admin User with the **Product Administrator** role. If your user account is assigned to a custom Admin User Role, your ability to view, modify, or execute actions on this page are based on the permissions specified for that role.
2. From the main menu, select **Encryption**, and then click the **Encrypted Folders** link.
3. Helpsystems recommends encrypting as many locations accessed by GoAnywhere MFT as possible.

Folder Restrictions

To prevent encryption of vital GoAnywhere system resources, GoAnywhere has restrictions on which folders can be encrypted:

- You cannot encrypt a root drive. For example, you would not be able to encrypt C:\.
- You cannot encrypt the GoAnywhere install directory, or any parent directory of the install directory.
- The WebDocs and Workspace directories are the only directories within the GoAnywhere install directory where encryption is allowed. The locations of these folders are configured on the Domain.
- You cannot encrypt a child folder of a directory that is already encrypted.
- You cannot encrypt a parent folder of a directory that contains an encrypted child directory.

NOTE:

When using encrypted folders in GoAnywhere, data at rest can only be accessed through the GoAnywhere application.

Master Encryption Keys

GoAnywhere MFT ships with a product encryption key that, by default, is used to encrypt passwords, keys, and other sensitive data. The Master Encryption Keys feature allows administrators to create and manage master keys. The most recently created Master

Encryption Key will always be set to the 'current' key and will be labeled as such in the list of keys.

To manage master encryption keys:

1. Log in as an Admin User with both **Product Administrator** and **Security Officer** roles. If your user account is assigned to a custom Admin User Role, your ability to view, modify, or execute actions on this page are based on the permissions specified for that role.
2. Select **Encryption** from the main menu bar and then click the **Master Encryption Keys** link.

HelpSystems recommends creating a new Master Encryption Key. Rotate Master Encryption Keys as directed by your security policy.

System

Security Settings

The following section provides all recommended settings for the Security Settings page. Only fields and options with recommended settings will be addressed.

The Security Settings option is only available to Admin Users with the **Security Officer** role. If your user account is assigned to a custom Admin User Role, your ability to view, modify, or execute actions on this page are based on the permissions specified for that role.

Any changes to Security Settings are implemented globally throughout GoAnywhere MFT.

From the main menu bar, select **System**, and then click **Security Settings**.

NOTE: Changes to Security Settings requires a restart of GoAnywhere MFT.

FIPS 140-2 Compliance

Enable FIPS 140-2 Compliance Mode

Enabling FIPS mode is optional but strongly recommended.

SSL/TLS Cipher Suites in FIPS 140-2 Compliance Mode

The following table lists which SSL cipher suites, supplied by Bouncy Castle, are used for FTP, FTPS, HTTPS, AS2, SSL, SMTPS, GoFast, and Agent communications, as well as database connections and User authentication over SSL (LDAPS). The table also lists compatibility with SSLv3, TLSv1, TLSv1.1, and TLSv1.2.

Cipher Suite Name	SSLv3	TLSv1	TLSv1.1	TLSv1.2
TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384	N	N	N	Y
TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256	N	N	N	Y
TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA384	N	N	N	Y
TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256	N	N	N	Y

TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA	N	Y	Y	Y
TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA	N	Y	Y	Y
TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256	N	N	N	Y
TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256	N	N	N	Y
TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA	N	Y	Y	Y
TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA	N	Y	Y	Y
TLS_RSA_WITH_AES_256_GCM_SHA384	N	N	N	Y
TLS_RSA_WITH_AES_128_GCM_SHA256	N	N	N	Y
TLS_RSA_WITH_AES_256_CBC_SHA256	N	N	N	Y
TLS_RSA_WITH_AES_128_CBC_SHA256	N	N	N	Y
TLS_RSA_WITH_AES_256_CBC_SHA	Y	Y	Y	Y
TLS_RSA_WITH_AES_128_CBC_SHA	Y	Y	Y	Y

TIP:

The server operating system and Java Virtual Machine version may limit which cipher suites are used by your system when FIPS 140-2 Compliance Mode is enabled.

SSH Algorithms in FIPS 140-2 Compliance Mode

The following SSH algorithms, supplied by Bouncy Castle, are used for SFTP and SCP communications.

Key Exchange

- DIFFIE-HELLMAN-GROUP14-SHA1
- ECDH-SHA2-NISTP256
- ECDH-SHA2-NISTP384
- ECDH-SHA2-NISTP521

Ciphers

- AES128-CBC
- AES192-CBC
- AES256-CBC
- AES128-CTR
- AES192-CTR
- AES256-CTR

Mac

- HMAC-SHA2-512
 - HMAC-SHA2-256
 - HMAC-SHA1
 - HMAC-SHA1-96
-

Algorithms Tab

Specify the SSL/TLS protocol versions and cipher suites to allow globally. Some allowed protocols and cipher suites may forcibly be disabled depending on your JVM and security provider.

	Disabled		Allowed
Protocols	SSLv2Hello	<div>→</div> <div>↔</div> <div>←</div> <div>⇐</div>	TLSv1.2
	SSLv3		
	TLSv1		
	TLSv1.1		
	TLSv1.3		
Cipher Suites			TLS_AES_128_GCM_SHA256 TLS_AES_256_GCM_SHA384 TLS_DHE_DSS_WITH_AES_128_CBC_SHA TLS_DHE_DSS_WITH_AES_128_CBC_SHA256 TLS_DHE_DSS_WITH_AES_128_GCM_SHA256 TLS_DHE_DSS_WITH_AES_256_CBC_SHA TLS_DHE_DSS_WITH_AES_256_CBC_SHA256 TLS_DHE_DSS_WITH_AES_256_GCM_SHA384 TLS_DHE_RSA_WITH_AES_128_CBC_SHA

Protocols

Enable only TLSv1.2.

NOTE:

Connecting to outdated servers may cause connectivity issues.

Validation Tab

Certificate Validation
Specify checks to enforce when validating client, server, and email certificates.

CA Basic Constraints Validation	<input checked="" type="checkbox"/> Client Certificates	<input checked="" type="checkbox"/> Server Certificates	<input checked="" type="checkbox"/> Email Certificates
Date Validation	<input checked="" type="checkbox"/> Client Certificates	<input checked="" type="checkbox"/> Server Certificates	<input checked="" type="checkbox"/> Email Certificates
Extended Key Usage Validation	<input checked="" type="checkbox"/> Client Certificates	<input checked="" type="checkbox"/> Server Certificates	<input checked="" type="checkbox"/> Email Certificates
Certificate Revocation Lists (CRL)	<input checked="" type="checkbox"/> Client Certificates	<input checked="" type="checkbox"/> Server Certificates	<input checked="" type="checkbox"/> Email Certificates

Refresh Interval Minutes

URLs [Add URL](#)

URL
✗ <input type="text" value="https://pki.google.com/GIAG2.crl"/>

Hostname Verification
Specify whether or not to strictly enforce hostname verification. If set to "Yes", the hostname for all SSL/TLS connections must match any Subject Alternative Name (SAN) IP/DNS entries or the Subject Common Name (CN) on the server's certificate. With Strict Hostname Verification, wildcards "*" may only comprise the entire left-most portion of a SAN DNS entry or CN (*.example.com). If set to "No", protocol specific hostname verification will be performed. Protocol specific verification is less strict and varies depending on the protocol utilizing SSL/TLS encryption.

Strict Hostname Verification ☒ Yes ☐ No

Implicit Trust
Specify whether or not to allow implicit trust for certain connections that support this configuration. If set to "No", implicit trust will be globally disabled and all connections will be required to validate certificate or public key information.

Allow Implicit Trust (SSL/TLS) ☐ Yes ☒ No

Allow Implicit Trust (SSH) ☐ Yes ☒ No

Certificate Validation

CA Basic Constraints Validation

Enable all certificate checks.

Date Validation

Enable all certificate checks.

Extended Key Usage Validation

Enable all certificate checks.

NOTE:

If running in a clustered system with Agents, rotate the Agent server key to an SSL certificate that has been generated with the Client and Server Extended Key Usage attributes defined.

NOTE:

If enabling client SSL certificate validation, make sure that any users authenticating with SSL certificates are using certificates that have the Client Extended Key Usage attribute defined.

Certificate Revocation Lists (CRL)

Enable all certificate checks. This helps prevent man-in-the-middle attacks. Consult your security team to determine which CRL to pull from.

Refresh Interval

Set to default value of 5 minutes.

Hostname Verification

Strict Hostname Verification

Enable.

Implicit Trust

Allow Implicit Trust (SSL/TLS)

Disable. This helps prevent man-in-the-middle attacks.

Allow Implicit Trust (SSH)

Disable. This helps prevent man-in-the-middle attacks.

Global Settings

The following section provides all recommendations for Global Settings. Only fields and options with recommended settings will be addressed.

Global Settings are used to control the overall behavior and attributes of GoAnywhere. These settings can be viewed and modified by an Admin User with the **Product Administrator** role. If your user account is assigned to a custom Admin User Role, your ability to view, modify, or execute actions on this page are based on the permissions specified for that role.

From the main menu, select **System**, and then click the **Global Settings** link.

SMTP Tab

Connect to an SSL enabled port. Configure the SMTP settings to use User Name and Password whenever possible.

SMS Tab

When using SMS, refer to your SMS provider for best practices.

Admin Configuration

The following section provides all recommended settings for the Admin Configuration page. Only fields and options with recommended settings will be addressed.

To manage Admin Configuration:

1. Log in as an Admin User with the **Product Administrator** role. If your user account is assigned to a custom Admin User Role, your ability to view, modify, or execute actions on this page are based on the permissions specified for that role.
2. From the main menu, select **System** and then click the **Admin Server** link. From the Admin Server page, click **Edit** to edit the Admin Configuration.

Listener

General Tab

Server Header

Set the Server Header name to something generic (such as 'Null', 'None', or 'Web Server'). Information gathered from the header name can help attackers in malicious activities.

SSL Tab

The screenshot displays the SSL configuration interface with the following fields and options:

- SSL Enabled:** A dropdown menu set to "Yes".
- SSL Protocol:** A text input field containing "TLS".
- Enabled SSL Protocols:** An empty text input field.
- Algorithm:** An empty text input field.
- Client Authentication:** A dropdown menu.
- Enabled Cipher Suites:** A section with two columns:
 - Available:** A list of cipher suites including TLS_AES_128_GCM_SHA256, TLS_AES_256_GCM_SHA384, TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384, TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256, TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384, TLS_RSA_WITH_AES_256_GCM_SHA384, TLS_ECDH_ECDSA_WITH_AES_256_GCM_SHA384, TLS_ECDH_RSA_WITH_AES_256_GCM_SHA384, TLS_DHE_RSA_WITH_AES_256_GCM_SHA384, and TLS_DHE_DSS_WITH_AES_256_GCM_SHA384.
 - Selected:** An empty list box.
 - Navigation buttons: "+", "→", "←", and "-".
- Certificate Location:** A dropdown menu set to "System Key Vault".
- Key Name:** A text input field containing "goanywhere-sample".
- Key Password:** An empty text input field.
- Export Head Certificate:** A button.

A note at the bottom right states: "JVM Default Cipher Suites are used if none are selected".

SSL Enabled

Enable. It is best practice to enable SSL on Listeners unless redirecting from HTTP to HTTPS.

SSL Protocol

Use the default, TLS protocol.

Enabled SSL Protocols

Leave this field blank. Settings will be inherited from the Global Security Settings page.

Client Authentication

If all users are authenticating with certificates, set this option to 'Required'. If only some users are authenticating with certificates, use 'Optional'. Otherwise, use 'None'.

Enabled Cipher Suites

Use this list to further limit the protocol specific Cipher Suites beyond those specified in the Security Settings.

Certificate Location

Import your company's private SSL key into the Key Management System and apply them to the HTTPS listener. If a signed certificate is not available, create an SSL certificate and apply it. Use the latest version of SSL certificate as possible and the largest key size possible. If using certificate version 3, be sure that the certificate extended key usage is set to an SSL/TLS server. See the HTTPS Certificate Quick Start Guide in the GoAnywhere Admin User Guide for more information.

Redirection Tab

HTTP/HTTPS traffic can be automatically redirected to the intended protocol, host and/or port. The redirect process substitutes the appropriate portion of the URL ([protocol]://[host][:port]).

To securely redirect from HTTP to HTTPS, set up an HTTP listener and enable redirection on that listener. Configure the redirection fields as necessary, set the redirection protocol as HTTPS, and redirect to the existing HTTPS listener.

Database Configuration

The Database Configuration page displays the current database configuration and provides options to edit the current database configuration or migrate the embedded GoAnywhere database to an external database.

To manage the database:

1. Log in as an Admin User with the **Product Administrator** role.
2. From the main menu, select **System**, and then click the **Database Configuration** link.

By default, GoAnywhere stores its configuration settings and application data in an embedded Derby database. HelpSystems recommends switching to an external database

so that a database administrator can manage database security. Enable SSL communication with the database if possible.

WARNING:

Only perform the database switch when no other users are using GoAnywhere. The migration will stop Monitors, Scheduled Jobs, Service Level Agreements, and Projects from executing. Additionally, all services, Web User sessions, and the GoAnywhere Gateway connection will be stopped.

See the Switch Database topic in the GoAnywhere User Guide for instructions on how to switch databases.

NOTE:

You need to export the internal database's certificate to a local file-based trust store, then specify that trust store in your JDBC URL *Example: &trustStore=C:\Program Files\HelpSystems\GoAnywhere\userdata\keys\x509\trustedCertificates.jks&trustStorePassword=goanywhere*

System Alerts

The following section provides recommendations for System Alerts settings. Only fields and options with recommended settings will be addressed. The System Alert settings do not directly affect the security of the application, however they can alert administrators to potential security issues.

When system alerts are enabled, GoAnywhere can email Product Administrators when the system is started, shut down, when memory is reaching a set threshold, the GoAnywhere license is set to expire, or when changes are made to a GoAnywhere Cluster. System Alerts are useful in pointing to stability and security issues.

To modify System Alerts:

1. Log in as an Admin User with the **Product Administrator** role.
2. From the main menu, select **System**, and then click the **System Alerts** link.

General Settings

System Alerts Enabled

Enable.

Administration

GoAnywhere Started

Notify Product Administrators
Enable.

GoAnywhere Shutdown

Notify Product Administrators
Enable.

JVM Memory

Available Memory Less Than
Set a memory limit.

Notify Product Administrators
Enable.

Notify Additional Email Addresses
Enable this feature if additional users need to be notified.

License Expiring

License Expiring Within
Set a time limit.

Notify Product Administrators
Enable.

Web Users

Web User Deactivated

Notify Web User Managers
Enable.

Certificates

Certificate Expiring

Certificate Expiring Within
Set a time limit.

Notify Key Managers
Enable.

PGP Keys

PGP key Expiring

PGP Key Expiring Within

Set a time limit.

Notify Key Managers

Enable.

Triggers

Trigger Failed

Notify Trigger Managers

Enable.

Gateway

Gateway Connected

Notify Product Administrators

Enable.

Gateway Disconnected

Notify Product Administrators

Enable.

Clustering

Cluster Membership Changes

Notify Product Administrators

Enable.

IP Filter

The IP Filter page provides the options to create and configure the global IP filter list. To manage IP filters, log in as an Admin User with the **Security Officer** role.

From the main menu, select **System**, and then click the **IP Filter** link.

Set 'IP Filtered Enabled' to true.

Filter Entries

As a best practice, create a list of allowed addresses.

IP Block Listing

The following section provides all recommendations for IP Block Listing settings. Only fields and options with recommended settings will be addressed.

The Automatic IP Block List feature in GoAnywhere monitors the active services for repeated unsuccessful access attempts. The Automatic IP Block List can detect brute-force and denial of service (DoS) attacks, as well as monitor for malicious user names.

To manage Automatic IP Block Lists:

1. Log in as an Admin User with the **Security Officer** role.
2. From the main menu, select **System**, and then click the **Automatic IP Block List** link.

Automatic IP Block List

Automatic Block List Enabled

Enable this feature.

Brute-force Attack Monitor Enabled

Enable the brute-force monitor and set the Sensitivity to 'Very High' with a Ban Type of 'Permanent'.

DoS Attack Monitor Enabled

Enable the DoS attack monitor and set the Sensitivity to 'Very High' with a Ban Type of 'Permanent'.

Malicious User Name Monitor Enabled

Enable malicious user name monitoring and add a list of common user names that you are not using within the application. (root, admin, administrator, ec2-user, etc.).

Automatic IP Block List Exemptions

The Automatic IP Block List Exemptions feature in GoAnywhere excludes specified IP addresses from being block listed after repeated unsuccessful access attempts.

To manage Automatic IP Block Lists Exemptions, log in as an Admin User with the **Security Officer** role. If your user account is assigned to a custom Admin User Role, your ability to view, modify, or execute actions on this page are based on the permissions specified for that role.

From the main menu, select **System**, and then click the **Automatic IP Block List** link. Click the **Exemptions** icon Exemptions button on the Automatic IP Block List page.

Services

GoAnywhere services are used for inbound connections from your trading partners, customers, employees, and remote sites. The available services (protocols) are HTTPS, AS2, AS4, FTP, SFTP, GoFast, Agents, and PeSIT.

HTTPS/AS2/AS4

The following section provides the recommended settings for hardening the HTTPS/AS2/AS4 Service. Only fields and options with recommended settings will be addressed.

To manage the HTTPS/AS2/AS4 Service:

1. Log in as an Admin User with the **Product Administrator** role. If your user account is assigned to a custom Admin User Role, your ability to view, modify, or execute actions on this page are based on the permissions specified for that role.
2. From the main menu bar, select **Services** and then click the **Service Manager** link.
3. Click **Action** next to the HTTPS Service, and then click **Edit**.

Web Client

Enabled	<input checked="" type="checkbox"/>
Allow Browsers to Save Login Credentials	<input type="checkbox"/>
Allow Session ID in URL	<input type="checkbox"/>
Allow Embedding within an IFrame	<input type="checkbox"/>
Allow Embedding Secure Forms From	<input type="text" value="No Website"/>
HTTP Strict Transport Security	
Including this header will instruct supported browsers to prevent all HTTP communication by enforcing HTTPS and blocking users from overriding invalid certificate warnings.	
Include Header	<input checked="" type="checkbox"/>
Maximum Age *	<input type="text" value="86400"/> Seconds
Include Subdomains	<input type="checkbox"/>
Include Preload Option	<input type="checkbox"/>
HTTP Content Security Policy	
The content security policy mitigates potential threats by restricting which domains content can be loaded from.	
Policy	<input type="text" value="Default"/>
<pre>default-src 'self' *.goanywhere.com; script-src 'self' 'unsafe-inline' 'unsafe-eval'; style-src 'self' 'unsafe-inline'; img-src * data: blob;;</pre>	

Enabled

Enable the Web Client if you plan to use it. If not, disable this feature.

Allow Browsers to Save Login Credentials

Disable this feature. This will prevent browsers from storing credentials for this web page. Saved login credentials can increase the chance of stolen or misused user privileges.

Allow Session ID in URL

Disable this feature. This will prevent the URL from displaying the Session ID. Information gathered from exposed Session IDs can help attackers in malicious activities.

HTTP Strict Transport Security (HSTS)

Enabling the HTTP Strict Transport Security (HSTS) header will instruct supported browsers to prevent all HTTP communication to GoAnywhere MFT by enforcing HTTPS and blocking users from overriding invalid certificate warnings.

Include Header

Enabled

Maximum Age

Set the maximum age to greater than 10368000 seconds (120 days).

HTTP Content Security Policy (CSP)

The Content Security Policy (CSP) response header allows Admin Users to control which resources GoAnywhere is allowed to load for a given page. The CSP mitigates potential threats by restricting which domains content can be loaded from.

Policy

Begin with 'Default' setting. Consult your internal security team and customize as needed.

NOTE:

Adjusting the CSP policy can impact application functionality. Please test all changes before applying them to a production environment.

Secure Folders Tab

Secure Folders allows Web Users to work with authorized folders and files on the network through the HTTPS Web Client.

Enable Java Applet

Disable this feature.

Enable Quick Downloads

Disable this feature if you do not plan to use it.

Enable Quick Uploads

Disable this feature if you do not plan to use it.

User Interface Tab

Help File/URL

If the Help link will open a document (for example, a PDF, text file, or HTML document), that file must be copied to the `[installdirectory]/ghttpsroot/custom` folder, where `[installdirectory]` is the installation directory of GoAnywhere. Valid file types are txt, xhtml, htm, html, pdf, doc, docx, rtf, and odt.

NOTE:

Even though file types will be validated, HelpSystems recommends following the principle of least privilege when determining who has access to the **ghttpsroot** directory.

HTTPS

The screenshot shows the 'HTTPS' configuration tab in the GoAnywhere interface. It contains several settings:

- Maximum Upload File Size ***: A numeric input field set to 4096 MB.
- Allow Files with No Extension**: An unchecked checkbox.
- Allow Files with an Extension**: A checked checkbox.
- File Extension Filter**: A dropdown menu set to 'Accept Extensions Defined Below' and a checked 'Case Sensitive' checkbox.
- A text area for file extensions containing 'txt.csv' with a '1993 Characters Remaining' indicator.
- ASCII Mode File Name Patterns**: An empty text area with a '2000 Characters Remaining' indicator.
- Download as Zip**: A section with an 'Enabled' checkbox checked.
- File Name Pattern ***: A text input field containing 'documents_\${yyyyMMdd}' and a 'Test' button.
- File Limit**: A numeric input field set to 1000.

Maximum Upload File Size

Configuring a maximum upload size can help prevent attacks that consume server resources. Therefore, limit the maximum upload size according to your company's needs and security policy. HelpSystems also recommends limiting disk space for Web Users and Web User Groups to help prevent this type of attack.

Allow Files with No Extension

HelpSystems recommends that you disable this feature, as this could help prevent the upload of malicious files.

Allow Files with an Extension

HelpSystems recommends that you enable this feature. Most valid file uploads will include a file extension. In addition, enabling this feature along with choosing a File Extension Filter allows GoAnywhere MFT to prevent unwanted files from being uploaded.

File Extension Filter

This text area allows you to list the file types that are allowed to be uploaded via GoAnywhere MFT. Limiting allowed file types can help prevent the upload of malicious files.

NOTE: Type all file extensions without a period (.), separate them with commas, and do not add line breaks or spaces (for example, if you want to allow only .txt, .xls, .xlsx and .csv files, type: `txt,xls,xlsx,csv`).

HelpSystems recommends choosing valid file extensions according to your company's needs and security policy.

AS2

The settings on the AS2 tab configure the identity, security, and file restrictions for AS2 communications. The AS2 service supports multiple AS2 Recipients, each with their own AS2 ID, certificate alias, upload folder destinations, MDN receipts, and message security.

AS2 General Tab

Enabled <input checked="" type="checkbox"/>

Enabled

Enable this Service only if you intend to use it.

AS2 Recipients

General	MDN (Receipts)	Message Security
AS2 ID * <input type="text" value="MyCompanyID"/>		
Default Upload Folder <input type="text"/>		
When File Exists <input type="text" value="Rename"/> ▼		
Message Decryption		
Key Location <input type="text" value="System Key Vault"/> ▼		
Key Name <input type="text" value="GHTTPS"/> ▼		
Key Password <input type="password" value="....."/>		

Message Decryption

Specify the key used to decrypt incoming messages. The corresponding certificate should be sent to all Web Users who will be sending AS2 messages to GoAnywhere MFT.

Key Location

Specify the key used to decrypt incoming messages. Use the System Key vault whenever possible. RSA keys with a key size of 2048 bits or larger are recommended. The corresponding certificate should be sent to all Web Users who will be sending AS2 messages to GoAnywhere. Use a dedicated SSL certificate for message decryption.

Keep Receipts

Enable

MDN Signature

Specify the location and name of the private key that will be used to sign the AS2 message receipt. This ensures nonrepudiation.

Key Location

Use a dedicated SSL certificate for message signatures.

Message Security Tab

Require Encryption	<input checked="" type="checkbox"/>
Require Signature	<input checked="" type="checkbox"/>
Require Authentication	<input checked="" type="checkbox"/>

Require Encryption

Enable this feature. Messages sent without encryption will be denied and will result in an error.

Require Signature

Enable this feature. Messages sent without a signature will be denied and will result in an error.

Require Authentication

Enable this feature. Messages sent without requiring authentication will be denied and will result in an error.

AS4

General Tab

Only enable the AS4 Service if you plan to use it.

Reception Awareness Tab

Set the **Maximum receipt Wait Time** as low as possible without triggering errors. A low wait time gives attackers less time to fake a response.

AS4 Message Channels

If you are using a Message Channel that does not have subchannels enabled, assign access to a single user. This ensures that the messages placed in this channel are sent to the correct recipient and prevents data leaks to non-privileged users.

Server

Listener

Server Header

Set the Server Header name to something generic (such as 'Null', 'None', or 'Web Server'). Information gathered from the header name can help attackers in malicious activities.

SSL Tab

The screenshot shows the SSL configuration interface with the following fields and options:

- SSL Enabled:** A dropdown menu set to "Yes".
- SSL Protocol:** A text input field containing "TLS".
- Enabled SSL Protocols:** An empty text input field.
- Algorithm:** An empty text input field.
- Client Authentication:** A dropdown menu.
- Enabled Cipher Suites:** A section with two columns:
 - Available:** A list of cipher suites including TLS_AES_128_GCM_SHA256, TLS_AES_256_GCM_SHA384, TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384, TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256, TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384, TLS_RSA_WITH_AES_256_GCM_SHA384, TLS_ECDH_ECDSA_WITH_AES_256_GCM_SHA384, TLS_ECDH_RSA_WITH_AES_256_GCM_SHA384, TLS_DHE_RSA_WITH_AES_256_GCM_SHA384, and TLS_DHE_DSS_WITH_AES_256_GCM_SHA384.
 - Selected:** An empty list box.
 - Navigation buttons: "+", "→", "←", and "-".
- Certificate Location:** A dropdown menu set to "System Key Vault".
- Key Name:** A text input field containing "goanywhere-sample".
- Key Password:** An empty text input field.
- Export Head Certificate:** A button.
- Footer note:** "JVM Default Cipher Suites are used if none are selected".

SSL Enabled

Enable. It is best practice enable SSL on Listeners unless redirecting from HTTP to HTTPS.

SSL Protocol

Use the default, TLS protocol. SSL is a deprecated protocol. This field is inherited from the System Security Settings.

Enabled SSL Protocols

Leave this field blank. Settings will be inherited from the Global Security Settings page.

Client Authentication

If all users are authenticating with certificates, set this option to 'Required'. If only some users are authenticating with certificates, use 'Optional'. Otherwise, use 'None'.

Enabled Cipher Suites

Use this list to further limit the protocol specific Cipher Suites beyond those specified in the Global Security Settings.

Certificate Location

Import your company's private SSL key into the Key Management System and apply them to the HTTPS listener. If a signed certificate is not available, create an SSL certificate and apply it. Use the latest version of SSL certificate as possible and the largest key size possible. If using certificate version 3, be sure that the certificate extended key usage is set to an SSL/TLS server. See the HTTPS Certificate Quick Start Guide in the GoAnywhere Admin User Guide for more information.

Redirection Tab

HTTP/HTTPS traffic can be automatically redirected to the intended protocol, host and/or port. The redirect process substitutes the appropriate portion of the URL ([protocol]://[host][:port]).

To securely redirect from HTTP to HTTPS, set up an HTTP listener and enable redirection on that listener. Configure the redirection fields as necessary, set the redirection protocol as HTTPS, and redirect to the existing HTTPS listener.

FTP

The following section provides all recommended settings for hardening the FTP Service. Only fields and options with recommended settings will be addressed.

To manage the FTP Service:

1. Log in as an Admin User with the **Product Administrator** role. If your user account is assigned to a custom Admin User Role, your ability to view, modify, or execute actions on this page are based on the permissions specified for that role.
2. From the main menu bar, select **Services** and then click the **Service Manager** link.
3. Click **Action** next to the FTP Service, and then click **Edit**.

Upload Restrictions

Upload Restrictions

Allow Files with No Extension ☐

Allow Files with an Extension ☒

File Extension Filter

Accept Extensions Defined Below ☒ Case Sensitive

txt,xls

1993 Characters Remaining

Allow Files with No Extension

HelpSystems recommends that you disable this feature, as this could help prevent the upload of malicious files.

Allow Files with an Extension

HelpSystems recommends that you enable this feature. Most valid file uploads will include a file extension. In addition, enabling this feature along with choosing a File Extension Filter allows GoAnywhere MFT to prevent unwanted files from being uploaded.

File Extension Filter

This text area allows you to list the file types that are allowed to be uploaded via GoAnywhere MFT. Limiting allowed file types can help prevent the upload of malicious files.

NOTE: Type all file extensions without a period (.), separate them with commas, and do not add line breaks or spaces (for example, if you want to allow only .txt, .xls, .xlsx and .csv files, type: **txt,xls,xlsx,csv**).

HelpSystems recommends choosing valid file extensions according to your company's needs and security policy.

Server

Listener

Name *	default
Port *	8021
Idle Timeout	0
Local Address	
Domain	
Force Encrypted Authentication	Yes
Encoding	

The listener specifies on which port the FTP service will monitor traffic.

Idle Timeout

Consult your security team to determine the optimal Idle Timeout setting.

Force Encrypted Authentication

Set to **Yes**, ensuring that credentials are always secure when authenticating with this server.

Explicit SSL

SSL Protocol	TLS													
Enabled SSL Protocols														
Client Authentication	Required													
Enabled Cipher Suites	<table border="1"> <thead> <tr> <th>Available</th> </tr> </thead> <tbody> <tr><td>TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384</td></tr> <tr><td>TLS_RSA_WITH_AES_256_CBC_SHA256</td></tr> <tr><td>TLS_ECDH_ECDSA_WITH_AES_256_CBC_SHA384</td></tr> <tr><td>TLS_ECDH_RSA_WITH_AES_256_CBC_SHA384</td></tr> <tr><td>TLS_DHE_RSA_WITH_AES_256_CBC_SHA256</td></tr> <tr><td>TLS_DHE_DSS_WITH_AES_256_CBC_SHA256</td></tr> <tr><td>TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA</td></tr> <tr><td>TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA</td></tr> <tr><td>TLS_RSA_WITH_AES_256_CBC_SHA</td></tr> </tbody> </table>	Available	TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384	TLS_RSA_WITH_AES_256_CBC_SHA256	TLS_ECDH_ECDSA_WITH_AES_256_CBC_SHA384	TLS_ECDH_RSA_WITH_AES_256_CBC_SHA384	TLS_DHE_RSA_WITH_AES_256_CBC_SHA256	TLS_DHE_DSS_WITH_AES_256_CBC_SHA256	TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA	TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA	TLS_RSA_WITH_AES_256_CBC_SHA	<table border="1"> <thead> <tr> <th>Selected</th> </tr> </thead> <tbody> <tr><td>TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA384</td></tr> </tbody> </table>	Selected	TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA384
Available														
TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384														
TLS_RSA_WITH_AES_256_CBC_SHA256														
TLS_ECDH_ECDSA_WITH_AES_256_CBC_SHA384														
TLS_ECDH_RSA_WITH_AES_256_CBC_SHA384														
TLS_DHE_RSA_WITH_AES_256_CBC_SHA256														
TLS_DHE_DSS_WITH_AES_256_CBC_SHA256														
TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA														
TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA														
TLS_RSA_WITH_AES_256_CBC_SHA														
Selected														
TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA384														
	JVM Default Cipher Suites are used if none are selected													
CCC Enabled	<input type="checkbox"/>													
CCC Send Close Notify	<input type="checkbox"/>													
Certificate Location	System Key Vault													
Key Name	goanywhere-key	Export Head Certificate												
Key Password														

An Explicit SSL connection will start on any available FTP port. The Explicit SSL configuration verifies a connection is made and then requests and verifies an SSL connection before transmitting login or file data.

Enabled SSL Protocol

Leave this field blank. Settings will be inherited from the Global Security Settings page.

Client Authentication

If all users are authenticating with certificates, set this option to 'Required'. If only some users are authenticating with certificates, use 'Optional'. Otherwise, use 'None'.

Enabled Cipher Suites

Cipher Suites should be set globally on the Security Settings page. You can further limit the protocol specific Cipher Suites using this option.

CCC Enabled

Disable unless otherwise requested by your security team. If a Web User sends the CCC command, it terminates the encryption on the command channel and all subsequent FTP communication on the command channel will be transmitted in plain text.

Certificate Location

Import your company's private SSL key into the Key Management System and apply them to the FTP listener. If a signed certificate is not available, create an SSL certificate and apply it. Use the latest version of SSL certificate as possible and the largest key size possible. If using certificate version 3, be sure that the certificate extended key usage is set to an SSL/TLS server.

Data Connection

Idle Timeout	<input type="text" value="120"/>
Force Encrypted Data Channels	<input type="button" value="Yes"/>

Force Encrypted Data Channels

Set to Yes. This setting forces SSL/TLS encryption on the data channels and rejects any attempts at plain text data transfers.

Active

Enabled	<input type="button" value=""/>
Validate IP	<input type="button" value="Yes"/>
Local Address	<input type="text" value=""/>
Local Port	<input type="text" value="14000"/>

With an "active" Data Connection, the client computer connects to the server on the control port and specifies to the server which port it is listening on for the data. This can cause issues with a firewall on the client side as it may block the incoming data connection from the server.

Enabled

It is strongly recommended to use a passive data connection unless absolutely necessary.

Validate IP

Set to Yes. This option specifies if the server should check if the IP address for the data connection is the same as for the control port. If the IP is not valid, the connection will fail.

Passive

Local Address	<input type="text"/>
External Address	<input type="text"/>
Validate IP	<input type="text" value="Yes"/>
Ports	<input type="text" value="32101-32200"/>

In a passive Data Connection, the client computer initiates the connection while the host decides the control port, using a port range within the firewall rules.

Validate IP

Set to Yes. This option specifies if the server should check if the IP address for the data connection is the same as for the control port. If the IP is not valid, the connection will fail.

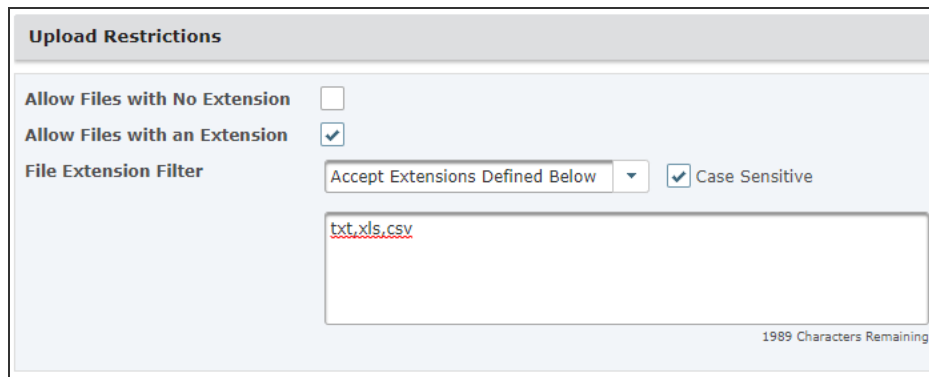
FTPS

The following section provides all recommended settings for hardening the FTPS Service. Only fields and options with recommended settings will be addressed.

To manage the FTPS Service:

1. Log in as an Admin User with the **Product Administrator** role. If your user account is assigned to a custom Admin User Role, your ability to view, modify, or execute actions on this page are based on the permissions specified for that role.
2. From the main menu bar, select **Services** and then click the **Service Manager** link.
3. Click **Action** next to the FTPS Service, and then click **Edit**.

Upload Restrictions



The screenshot shows a configuration window titled "Upload Restrictions". It contains the following elements:

- Allow Files with No Extension:** A checkbox that is currently unchecked.
- Allow Files with an Extension:** A checkbox that is currently checked.
- File Extension Filter:** A section containing:
 - A dropdown menu set to "Accept Extensions Defined Below".
 - A checked checkbox for "Case Sensitive".
 - A text input field containing the text "txt,xls,csv".
 - A character count at the bottom right of the text field: "1989 Characters Remaining".

Allow Files with No Extension

HelpSystems recommends that you disable this feature, as this could help prevent the upload of malicious files.

Allow Files with an Extension

HelpSystems recommends that you enable this feature. Most valid file uploads will include a file extension. In addition, enabling this feature along with choosing a File Extension Filter allows GoAnywhere MFT to prevent unwanted files from being uploaded.

File Extension Filter

This text area allows you to list the file types that are allowed to be uploaded via GoAnywhere MFT. Limiting allowed file types can help prevent the upload of malicious files.

NOTE: Type all file extensions without a period (.), separate them with commas, and do not add line breaks or spaces (for example, if you want to allow only .txt, .xls, .xlsx and .csv files, type: `txt,xls,xlsx,csv`).

HelpSystems recommends choosing valid file extensions according to your company's needs and security policy.

Server

Listener

The listener specifies on which port the FTPS service will monitor traffic.

Idle Timeout

Consult your security team to determine the optimal Idle Timeout setting.

Implicit SSL

SSL Protocol: TLS

Enabled SSL Protocols:

Client Authentication: Required

Enabled Cipher Suites:

Available	Selected
TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384	TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA384
TLS_RSA_WITH_AES_256_CBC_SHA256	
TLS_ECDH_ECDSA_WITH_AES_256_CBC_SHA384	
TLS_ECDH_RSA_WITH_AES_256_CBC_SHA384	
TLS_DHE_RSA_WITH_AES_256_CBC_SHA256	
TLS_DHE_DSS_WITH_AES_256_CBC_SHA256	
TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA	
TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA	
TLS_RSA_WITH_AES_256_CBC_SHA	

JVM Default Cipher Suites are used if none are selected

CCC Enabled: ☐

CCC Send Close Notify: ☐

Certificate Location: System Key Vault

Key Name: goanywhere-key Export Head Certificate

Key Password:

An Implicit SSL connection will start on any available FTP port. The Implicit SSL configuration verifies a connection is made and then requests and verifies an SSL connection before transmitting login or file data.

SSL Protocol

Use the default, TLS protocol. SSL is a deprecated protocol. This field is inherited from the System Security Settings.

Client Authentication

If all users are authenticating with certificates, set this option to 'Required'. If only some users are authenticating with certificates, use 'Optional'. Otherwise, use 'None'.

Enabled Cipher Suites

Use this list to further limit the protocol specific Cipher Suites beyond those specified in the Security Settings.

CCC Enabled

Disable unless otherwise requested by your security team. If a Web User sends the CCC command, it terminates the encryption on the command channel and all subsequent FTPS communication on the command channel will be transmitted in plain text.

Certificate Location

Import your company's private SSL key into the Key Management System and apply them to the FTPS listener. If a signed certificate is not available, create an SSL certificate and apply it. Use the latest version of SSL certificate as possible and the largest key size

possible. If using certificate version 3, be sure that the certificate extended key usage is set to an SSL/TLS server.

Data Connection

Force Encrypted Data Channels

Set to Yes. This setting forces SSL/TLS encryption on the data channels and rejects any attempts at plain text data transfers.

Active

Enabled	<input type="checkbox"/>
Validate IP	Yes <input type="checkbox"/>
Local Address	<input type="text"/>
Local Port	14001 <input type="button" value="▲"/> <input type="button" value="▼"/>

With an "active" Data Connection, the client computer connects to the server on the control port and specifies to the server which port it is listening on for the data. This can cause issues with a firewall on the client side as it may block the incoming data connection from the server.

Enabled

It is strongly recommended to use a 'Passive' data connection unless absolutely necessary.

Validate IP

Set to Yes. This option specifies if the server should check if the IP address for the data connection is the same as for the control port. If the IP is not valid, the connection will fail.

Passive

Local Address	<input type="text"/>
External Address	<input type="text"/>
Validate IP	Yes <input type="checkbox"/>
Ports	32101-32200 <input type="text"/>

In a passive Data Connection, the client computer initiates the connection while the host decides the control port, using a port range within the firewall rules.

Validate IP

Set to Yes. This option specifies if the server should check if the IP address for the data connection is the same as for the control port. If the IP is not valid, the connection will fail.

SFTP

The following section provides the recommended settings for hardening the SFTP Service. Only fields and options with recommended settings will be addressed.

To manage the SFTP Service:

1. Log in as an Admin User with the **Product Administrator** role. If your user account is assigned to a custom Admin User Role, your ability to view, modify, or execute actions on this page are based on the permissions specified for that role.
2. From the main menu bar, select **Services** and then click the **Service Manager** link.

Upload Restrictions

Limit Upload File Size

HelpSystems recommends that you enable this setting.

Maximum Upload File Size

Configuring a maximum upload size can help prevent attacks that consume server resources. Therefore, limit the maximum upload size according to your company's needs and security policy. HelpSystems also recommends limiting disk space for Web Users and Web User Groups to help prevent this type of attack.

Allow Files with No Extension

HelpSystems recommends that you disable this feature, as this could help prevent the upload of malicious files.

Allow Files with an Extension

HelpSystems recommends that you enable this feature. Most valid file uploads will include a file extension. In addition, enabling this feature along with choosing a File Extension Filter allows GoAnywhere MFT to prevent unwanted files from being uploaded.

File Extension Filter

This text area allows you to list the file types that are allowed to be uploaded via GoAnywhere MFT. Limiting allowed file types can help prevent the upload of malicious files.

NOTE: Type all file extensions without a period (.), separate them with commas, and do not add line breaks or spaces (for example, if you want to allow only .txt, .xls, .xlsx and .csv files, type: `txt,xls,xlsx,csv`).

HelpSystems recommends choosing valid file extensions according to your company's needs and security policy.

Server

SCP Enabled

Disable this option unless you are using it. Reducing the number of endpoints helps administrators focus security efforts.

Min DH Group Exchange Key Size

Use a 2048 minimum key size.

Enabled Key Exchange Algorithms

The recommended Key Exchange Algorithms are:

- DIFFIE-HELLMAN-GROUP14-SHA1
- ECDH-SHA2-NISTP256
- ECDH-SHA2-NISTP384
- ECDH-SHA2-NISTP521

NOTE:

Enable ECDSA keys to allow for more Public Key Signature Algorithms.

Enabled Cipher Algorithms

The recommended Cipher Algorithms are:

- AES128-CBC
 - AES192-CBC
-

- AES256-CBC
- AES128-CTR
- AES192-CTR
- AES256-CTR

Enabled Mac Algorithms

The recommended MAC Algorithms are:

- HMAC-SHA2-512
- HMAC-SHA2-256
- HMAC-SHA1

Enabled Compression Algorithms

Keep the default Compression Algorithms selected.

Software Version

The software name or version should be something generic such as 'Null', 'None', 'SFTP Server', etc. Information gathered from server header can help attackers in malicious activities.

Listener

Name *	<input type="text" value="default"/>
Port *	<input type="text" value="8022"/>
Local Address	<input type="text" value="0.0.0.0"/>
Domain	<input type="text"/>
Authentication Types Allowed	<input type="text" value="Either"/>

The listener specifies on which port the SFTP service will monitor traffic.

Authentication Types Allowed

Set to 'Either', and set Public Key and Password to required in the Web User configuration settings. Defer to company policy and your security team to make sure authentication types chosen are those allowed by your organization.

Host Keys

Generate a new SSH RSA or ECDSA key under the System Key Vault of size 2048 or greater and use it for the SFTP Service. Remove any DSA key in the configuration. DSA keys are not allowed when FIPS 140-2 mode is enabled.

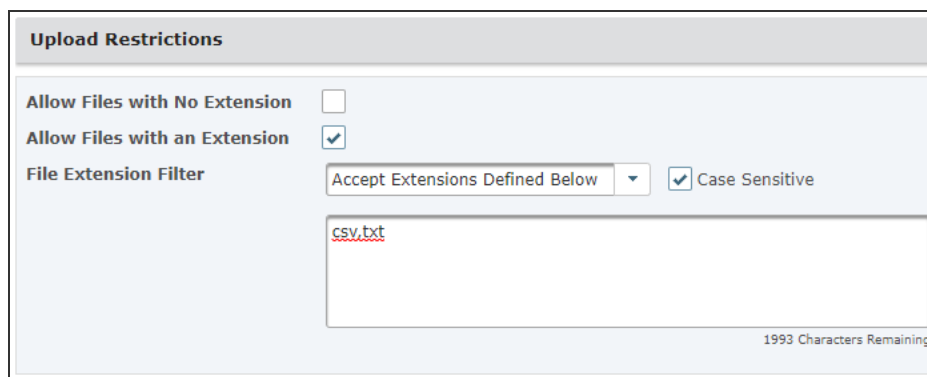
GoFast

The following section provides all recommended settings for hardening the GoFast Service. Only fields and options with recommended settings will be addressed.

To manage the GoFast Service:

1. Log in as an Admin User with the **Product Administrator** role. If your user account is assigned to a custom Admin User Role, your ability to view, modify, or execute actions on this page are based on the permissions specified for that role.
2. From the main menu bar, select **Services** and then click the **Service Manager** link.
3. Click **Action** next to the GoFast Service, and then click **Edit**.

Upload Restrictions



Allow Files with No Extension

HelpSystems recommends that you disable this feature, as this could help prevent the upload of malicious files.

Allow Files with an Extension

HelpSystems recommends that you enable this feature. Most valid file uploads will include a file extension. In addition, enabling this feature along with choosing a File Extension Filter allows GoAnywhere MFT to prevent unwanted files from being uploaded.

File Extension Filter

This text area allows you to list the file types that are allowed to be uploaded via GoAnywhere MFT. Limiting allowed file types can help prevent the upload of malicious files.

NOTE: Type all file extensions without a period (.), separate them with commas, and do not add line breaks or spaces (for example, if you want to allow only .txt, .xls, .xlsx and .csv files, type: `txt,xls,xlsx,csv`).

HelpSystems recommends choosing valid file extensions according to your company's needs and security policy.

Control Channel SSL

SSL Protocol:

Enabled SSL Protocols:

Client Authentication:

Enabled Cipher Suites:

Available	Selected
TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384	TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA384
TLS_RSA_WITH_AES_256_CBC_SHA256	
TLS_ECDH_ECDSA_WITH_AES_256_CBC_SHA384	
TLS_ECDH_RSA_WITH_AES_256_CBC_SHA384	
TLS_DHE_RSA_WITH_AES_256_CBC_SHA256	
TLS_DHE_DSS_WITH_AES_256_CBC_SHA256	
TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA	
TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA	
TLS_RSA_WITH_AES_256_CBC_SHA	

Certificate Location:

Key Name:

Key Password:

JVM Default Cipher Suites are used if none are selected

Enabled SSL Protocols

Leave this field blank. This setting is covered by the Global Security Settings.

Client Authentication

If all users are authenticating with certificates, set this option to 'Required'. If only some users are authenticating with certificates, use 'Optional'. Otherwise, use 'None'.

Enabled Cipher Suites

Use this option to limit the list of enabled Cipher Suites beyond those enabled in the Global Security Settings.

Certificate Location

Import your company's private SSL key into the Key Management System and apply it. If a signed certificate is not available, create an SSL certificate and apply it. Use the latest version of SSL certificate as possible and the largest key size possible. If using certificate version 3, be sure that the certificate extended key usage is set to an SSL/TLS server.

Agent Service

The following section provides all recommended settings for hardening the Agents Service. Only fields and options with recommended settings will be addressed.

To manage the Agent Service:

1. Log in as an Admin User with the **Product Administrator** role. If your user account is assigned to a custom Admin User Role, your ability to view, modify, or execute actions on this page are based on the permissions specified for that role.
2. From the main menu bar, select **Services** and then click the **Service Manager** link.
3. Click **Action** next to the Agent Service, and then click **Edit** .

Registration

Require Approval

It is best practice to require approval for all Agent registrations. This allows for a two-step process before an Agent can connect to the server.

Notify Agent Managers

Select this options so that administrators can monitor Agent registrations.

Server

SSL

SSL Protocol

Leave this field blank.

Enabled SSL Protocols

Leave this field blank. The default SSL/TLS for the JVM will be used. These settings can be changed on the Security Settings page.

NOTE:

Add other algorithms as needed from the Security Settings page.

Enabled Cipher Suites

Use this option to limit the list of enabled Cipher Suites beyond those enabled in the Security Settings.

PeSIT

The following section provides all recommended settings for hardening the PeSIT Service. Only fields and options with recommended settings will be addressed.

To manage the PeSIT Service:

1. Log in as an Admin User with the **Product Administrator** role. If your user account is assigned to a custom Admin User Role, your ability to view, modify, or execute actions on this page are based on the permissions specified for that role.
2. From the main menu bar, select **Services** and then click the **Service Manager** link.
3. Click **Action** next to the PeSIT Service, and then click **Edit**.

SSL

SSL Enabled

Enable.

Enabled SSL Protocol

Leave this field blank. Settings will be inherited from the Global Security Settings page.

NOTE:

Add other algorithms as needed from the Global Security Settings page.

Client Authentication

If all users are authenticating with certificates, set this option to 'Required'. If only some users are authenticating with certificates, use 'Optional'. Otherwise, use 'None'.

Enabled Cipher Suites

Cipher Suites should be set on the Global Security Settings page. You can further limit the protocol specific Cipher Suites using this option.

Key Name

Import your company's private SSL key into the Key Management System and apply them to the PeSIT listener. If a signed certificate is not available, create an SSL certificate and apply it. Use the latest version of SSL certificate as possible and the largest key size possible. If using certificate version 3, be sure that the certificate extended key usage is set to an SSL/TLS server.

GoAnywhere Gateway

The following section provides all recommended settings for hardening GoAnywhere Gateway. Only fields and options with recommended settings will be addressed.

To manage the GoAnywhere Gateway:

1. Log in as an Admin User with the **Product Administrator** role. If your user account is assigned to a custom Admin User Role, your ability to view, modify, or execute actions on this page are based on the permissions specified for that role.
2. From the main menu bar, select **Services** and then click the **Gateway Manager** link.

Gateway Manager

Gateway IP Filter and Log Rejected IP Addresses

Gateway IP Filter

Enable the Gateway IP Filter. This allows the gateway to filter client connections based on the IP Filter Allow List and Block List managed by GoAnywhere.

Log Rejected IP Address

Enable Log Rejected IP Addresses. GoAnywhere Gateway will log rejected IP addresses in the Gateway log file on the Gateway installation.

Gateway Configuration

Control Channel Security

SSL Enabled

Enable. It is best practice enable SSL on Listeners unless redirecting from HTTP to HTTPS.

Implicit SSL

Disable. This helps prevent man-in-the-middle attacks.

SSL Context Protocol

Enable only TLSv1.2.

NOTE:

Connecting to outdated GoAnywhere Gateway servers may cause connectivity issues.

Secure Mail Settings

The following section provides all recommended settings for hardening the Secure Mail feature. Only fields and options with recommended settings will be addressed.

To manage Secure Mail Settings:

1. Log in as an Admin User with the **Secure Mail Manager** role. If your user account is assigned to a custom Admin User Role, your ability to view, modify, or execute actions on this page are based on the permissions specified for that role.
2. From the main menu bar, select **Services** and then click the **Secure Mail, Settings** link.

General

Secure Mail Enabled

Enable Secure Mail only if it is actively being used.

File Limit per Package

Set the File Limit per Package with consideration to your disk space.

Send Package

Protection Level

Allowed Options	<input type="checkbox"/> URL Protected <input checked="" type="checkbox"/> Password Protected <input checked="" type="checkbox"/> Certified Delivery
Default	<div>Certified Delivery ▼</div>

Disable **URL Protected** and enable **Password Protected** and **Certified Delivery**.

Set the Default to **Certified Delivery**. When Certified Delivery is enabled, Web Users will be given an option to require recipients to register before they can access the message.

Password Generation

Allowed Options	<input checked="" type="checkbox"/> Generated Automatically <input type="checkbox"/> Manually Specified
Default	<div>Generated Automatically ▼</div>

Enable **Generated Automatically** and disable **Manually Specified**. Manually specified passwords can be set to a single character and are not as secure.

Set the Default to **Generated Automatically**.

Password Notification

Allowed Options	<input checked="" type="checkbox"/> Email <input checked="" type="checkbox"/> Text Message (SMS)
Default	<div>Text Message (SMS) ▼</div>
Send in Separate Email	<input checked="" type="checkbox"/>
Text Message (SMS) Format *	<div>`\${password}` is your Secure Mail password</div>

Enable **Email** and **Text Message (SMS)**.

Set the Default to **Text Message (SMS)** if SMS has been configured.

Enable **Send in Separate Email**.

Package Expiration

Enforce Range	<input checked="" type="checkbox"/>	<input type="text" value="1"/> to <input type="text" value="30"/> Days
Default		<input type="text" value="20"/> Days

Enable **Enforce Range**.

Set the Default to a number of days less than the desired enforced range.

Maximum Downloads

Enforce Range	<input checked="" type="checkbox"/>	<input type="text" value="1"/> to <input type="text" value="30"/> Downloads
Default		<input type="text" value="20"/> Downloads

Enable **Enforce Range**.

Set the Default to a number of days less than the desired enforced range.

Reply

Disable **Allowed**.

Set the Default to **No**. This prevents Web Users from receiving potentially risky files. In addition, enabling data loss prevention scanning using Triggers can further mitigate risk.

Request Files

Request Protection Level

Allowed Options	<input type="checkbox"/> URL Protected
	<input checked="" type="checkbox"/> Certified Delivery
Default	<input type="text" value="Certified Delivery"/>

Disable **URL Protected** and enable **Certified Delivery**.

Set the Default to the **Certified Delivery**. When Certified Delivery is enabled, Web Users will be given an option to require recipients to register before they can access the message.

Request Expiration

Enforce Range	<input checked="" type="checkbox"/> <input type="text" value="1"/> to <input type="text" value="30"/> Days
Default	<input type="text" value="20"/> Days

Enable **Enforce Range**.

Set the Default to a number of days less than the desired enforced range. Enforcing a range prevents links from being used in the future should a user's inbox be compromised.

Outlook Plugin Policy

Max File Size Options	<input checked="" type="radio"/> All file sizes <input type="radio"/> Files larger than <input type="text" value="1"/> MB <input type="radio"/> Never
Ask Before Sending	<input type="checkbox"/>
Enforce These Settings	<input checked="" type="checkbox"/>

Set the Max File Size Options to **All file Sizes**.

Disable **Ask Before Sending** and enable **Enforce These Settings**. Enforcing setting through the plugin policy ensures that all users adhere to the same settings when sending messages from Outlook.

Address Rules

Address Rules are used to define the Web User email addresses that are permitted to send Secure Mail, and to which recipient email addresses can be sent to.

Configure the address rules to permit the least number of email addresses necessary.

Secure Forms Settings

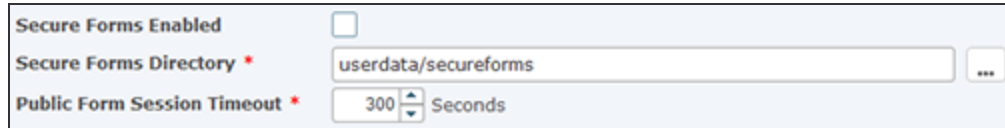
The following section provides all recommended settings for hardening Secure Forms.

To manage Secure Forms Settings:

1. Log in as an Admin User with the **Secure Forms Manager** role. If your user account is assigned to a custom Admin User Role, your ability to view, modify, or execute actions on this page are based on the permissions specified for that role.

2. From the main menu bar, select **Services** and then click the **Secure Forms, Settings** link.

Hardening Recommendations

A screenshot of a configuration panel for Secure Forms. It contains three settings: 'Secure Forms Enabled' with an unchecked checkbox, 'Secure Forms Directory' with a text input field containing 'userdata/secureforms' and a small '...' button to its right, and 'Public Form Session Timeout' with a numeric input field set to '300' and a 'Seconds' label.

If you plan to use Secure Forms, set a **Public Form Session Timeout**. If you are not using Secure Forms, uncheck **Secure Forms Enabled**.

Secure Form Configuration

The following section provides all recommended settings for Secure Form Configuration. Only fields and options with recommended settings will be addressed.

To configure a Secure Form:

1. Log in as an Admin User with the **Secure Forms Manager** role. If your user account is assigned to a custom Admin User Role, your ability to view, modify, or execute actions on this page are based on the permissions specified for that role.
2. From the main menu bar, select **Services > Secure Forms > Form Manager**.

Access

Enabling **Web Client Enabled** is recommended. Limit enabling access points to only those that are needed.

Disabling **Public Access** is recommended, but can be enabled if business needs require it. If Public Access is enabled, we recommend not allowing embedded forms.

Web Users

Assign Web Users using the principal of least privilege.

Web Groups

Assign Web Groups using the principal of least privilege.

Components

Utilize the Mask Input option to hide user input and the Encrypt Data option to ensure that sensitive data will not be shown in plaintext anywhere within the application.

Agent Configuration

The following section provides all recommended settings for Agent Configuration. Only fields and options with recommended settings will be addressed.

To manage Agents:

1. Log in as an Admin User with the **Agent Manager** role. If your user account is assigned to a custom Admin User Role, your ability to view, modify, or execute actions on this page are based on the permissions specified for that role.
2. From the main menu bar, select **Services** and then click the **Agents, Agent Settings** link.

General

Name *	<input type="text" value="Chicago_001"/>
Domain	<input type="text" value="Default"/>
Enabled	<input checked="" type="checkbox"/>
Description	<input type="text" value="Retail agent."/> <small>498 Characters Remaining</small>
Feature Set *	<input type="text" value="Standard"/> ▼

Registration

Specify a registration code below. An Agent device that registers using this registration code will be automatically registered to this Agent.

Registration Code *	<input type="text" value="60603-7"/>
----------------------------	--------------------------------------

Location

Country	<input type="text" value="United States"/> ▼
Address	<input type="text" value="1307 Main Street"/> <small>240 Characters Remaining</small>
City	<input type="text" value="Chicago"/>
State	<input type="text" value="Illinois"/> ▼
Postal Code	<input type="text" value="60603"/>

[Verify Location](#)

Use a unique registration code for each Agent. To automate for larger deployments, configure Agent settings through the Agent Service Listener. See the GoAnywhere MFT User Guide for more information.

Alerts

While not directly security related, alerting Agent Managers when an Agent goes offline can call attention to security issues.

Users

Admin Users

The following section provides all recommended settings for the Admin Users. Only fields and options with recommended settings will be addressed.

To add or edit Admin Users:

1. Log in as an Admin User with the **Security Officer** role. If your user account is assigned to a custom Admin User Role, your ability to view, modify, or execute actions on this page are based on the permissions specified for that role.
2. From the main menu bar, select **Users**, and then click the **Admin Users** link.

HelpSystems recommends creating a service account for all automated aspects of the application - Secure Forms, Triggers, Monitors, SLAs, etc. Avoid using 'root' or 'administrator' accounts for this purpose.

Admin User Fields

Two-Factor Authentication

Enable some form of two-factor authentication: RADIUS (for example, RSA SecurID and Duo), Time-based One-Time Password (for example, Google Authenticator), or GoAnywhere One-Time Password.

Roles

Assign roles using the principle of least privilege.

Groups

Assign groups using the principal of least privilege.

Domains

Assign domains using the principle of least privilege.

File Permissions

Limit Admin User folder access through the File Manager Settings. Use the principle of least privilege.

NOTE:

We recommend providing 'Read Only' access to Admin Users and only on an as-needed basis. Create Web Users (even for internal employees) for fully managed and audited access to files. Due to the sensitive nature of the **ghttpsroot** and **adminroot** directories, HelpSystems recommends practicing caution when determining who has access to these locations.

Admin User Groups

The following section provides all recommended settings for Admin User Groups.

To configure Admin User Groups:

1. Log in as an Admin User with the **Security Officer** role.
2. From the main menu bar, select **Users**, and then click the **Admin Users** link.

Be advised that any permissions given will be passed to all Admin Users within the Admin User Group.

Admin User Group Fields

Group Roles

Assign group member roles using the principle of least privilege.

Group Domains

Assign group member domains using the principle of least privilege.

Admin User Templates

The following section provides all recommended settings for Admin User Templates. Only fields and options with recommended settings will be addressed.

To configure Admin User Templates:

1. Log in as an Admin User with the **Security Officer** role.
2. From the main menu bar, select **Users**, and then click the **Admin User Templates** link.

Be advised that any permissions given at the group level will be passed to all Admin Users created with the Admin User Template.

Admin User Template Fields

Two-Factor Authentication

Enable some form of two-factor authentication: RADIUS (for example, RSA SecurID and Duo), Time-based One-Time Password (for example, Google Authenticator), or GoAnywhere One-Time Password.

Roles

Assign roles using the principle of least privilege.

Groups

Assign groups using the principle of least privilege.

Domains

Assign domains using the principle of least privilege.

File Permissions

Limit Admin User folder access through the File Manager Settings. Use the principle of least privilege.

Admin Security Settings

The following section provides all recommended settings for Admin Security Settings. Only fields and options with recommended settings will be addressed.

To manage Admin Security Settings:

1. Log in as an Admin User with the **Security Officer** role.
2. From the main menu bar, select **Users**, and then click **Admin Security Settings**.

General

Session Timeout (seconds) *	900
Allow Browsers to Save Login Credentials	<input type="checkbox"/>
Allow Viewing of Resource Passwords	<input type="checkbox"/>
Allow Session ID in URL	<input type="checkbox"/>
Allow Embedding within an IFrame	<input type="checkbox"/>
Default Resource Permissions for All Admin Users	<input type="checkbox"/> Edit <input type="checkbox"/> Delete <input type="checkbox"/> Export <input type="checkbox"/> Promote <input type="checkbox"/> Test <input type="checkbox"/> View <input type="checkbox"/> Use <input type="checkbox"/> Manage Permissions
File Manager Maximum Upload File Size *	4096 MB
HTTP Strict Transport Security	
Including this header will instruct supported browsers to prevent all HTTP communication by enforcing HTTPS and blocking users from overriding invalid certificate warnings.	
Include Header	<input checked="" type="checkbox"/>
Maximum Age *	86400 Seconds
Include Subdomains	<input checked="" type="checkbox"/>
Include Preload Option	<input checked="" type="checkbox"/>
HTTP Content Security Policy	
The content security policy mitigates potential threats by restricting which domains content can be loaded from.	
Policy	Default
<pre>default-src 'self' *.goanywhere.com https://maps.google.com https://csi.gstatic.com https://maps.googleapis.com https://maps.gstatic.com https://fonts.googleapis.com https://fonts.gstatic.com; img-src * data: blob;; script-src 'self' https://maps.google.com https://maps.googleapis.com 'unsafe-inline' 'unsafe-eval'; style-src 'self' https://fonts.googleapis.com 'unsafe-inline';</pre>	

Session Timeout

Set the session timeout according to company policy. OWASP recommends high risk applications be set from 120 to 300 seconds and 900 to 1800 for low risk applications.

Allow Browsers to Save Login Credentials

Disable this option to prevent login credentials from being used by another user.

Allow Viewing of Resource Passwords

Disable this option to prevent unwanted access to resource passwords.

Allow Session ID in URL

Disable this option. Information exposed in the URL can be used by intruders.

Allow Embedding within an IFrame

Disable this option to prevent click-jacking and cross frame reference attacks.

Default Resource Permissions for All Admin Users

Disable all options.

HTTP Strict Transport Security (HSTS)

Include Header

Enabled

Maximum Age

Leave this on the default setting unless your security team requires otherwise.

Include Subdomains

Enable this option.

Include Preload Option

HelpSystems recommends enabling this option if possible. See the GoAnywhere MFT User Guide for details.

HTTP Content Security Policy (CSP)

Policy

Start with the 'Default' setting and customize as needed. Consider consulting your internal security team and testing changes to the CSP before applying changes to a production environment.

Password Policy

Set password policy parameters in accordance with company password policy. Consult your internal security team for recommendations.

NOTE:

These settings only apply when using the GoAnywhere login method. If you use Active Directory to authenticate users, your password policy is managed by Active Directory.

Password Strength

Enforce Settings

Enforce password strength settings.

Minimum Password Length

Set the minimum password strength to 8.

Minimum Number of Upper Case Letters

Set a minimum of 1.

Minimum Number of Lower Case Letters

Set a minimum of 1.

Minimum Number of Digits

Set a minimum of 1.

Minimum Number of Special Characters

Set a minimum of 1.

Allowable Special Characters

Allow all special characters.

Password Age

Maximum Password Age

Do not set the Maximum Password Age to zero (0). The industry standard is 90 days. Consult your internal security team for recommendations.

NOTE:

Applying a Maximum Password Age can affect automated and service level accounts that use the internal login method.

Password History

Enforce Password History

Enable.

Disallow Reuse of the Last

Disallow reuse of passwords. The number should depend on the maximum age setting. Consult your internal security team for recommendations.

Web Users

The following section provides all recommended settings for the Web Users. Only fields and options with recommended settings will be addressed.

To configure Web Users:

1. Log in as an Admin User with the **Web User Manager** role.
2. From the main menu bar, select Users, and then click the **Web Users** link.

Authentication

Password Options

Enable 'Allow User to Change Password' if secure password polices are in place.

Password Expiration Interval

Leave this setting at 'Default' unless otherwise necessary. The Password Expiration Interval will be defined in the Web User Password Policy.

Authentication Types

It is best practice to use two-factor authentication, regardless of the protocol. Enable 'SAN/DN' whenever possible.

Groups

Assign Web User Groups using the principle of least privilege.

Features

Protocols	<input type="checkbox"/> AS2 <input type="checkbox"/> AS4 <input type="checkbox"/> FTP <input type="checkbox"/> FTPS <input type="checkbox"/> GoFast <input type="checkbox"/> HTTPS <input type="checkbox"/> PeSIT <input type="checkbox"/> SFTP
GoDrive	<input checked="" type="checkbox"/>
GoDrive Access	<input checked="" type="radio"/> Full Licensed User <input type="radio"/> View Only
GoDrive Disk Space Limited	<input type="text" value="Yes"/>
GoDrive Disk Space Limit *	<input type="text" value="5"/> <input type="text" value="GB"/>
GoDrive Create Links Allowed	<input type="checkbox"/>
Secure Folders	<input type="checkbox"/>
Secure Forms	<input type="checkbox"/>
Send Secure Mail	<input type="checkbox"/>
Send Invitations	<input type="checkbox"/>
View Activity Report	<input type="checkbox"/>
Maximum Concurrent Sessions	<input type="text" value="3"/>

Assign features using the principal of least privilege.

GoDrive Disk Space Limited

Set a reasonable GoDrive disk space limit.

Maximum Concurrent Sessions

Set a reasonable maximum number of concurrent sessions based upon user need and company security policy. This helps prevent denial of service attacks.

Folders

Assign folder permissions using the principle of least privilege.

NOTE:

Disk space limits can cause negative performance impacts in large scale environments.

Forms

Assign forms using the principle of least privilege.

IP Filter

Enable IP Filter

Enable this feature. These filters control which IP addresses or address ranges have access to the various protocols.

Filter Type

Enable 'Allow List'.

Time Limits

Disable Account When No Activity

Set to 'Default (As defined in the web user security settings).'

AS4

Pull Processing Modes

Signal Message Decryption

Use a unique key pair for each trading partner.

User Message Signature

Enable **Sign User Message**. Signed messages help ensure nonrepudiation.

User Message Encryption

Enable this feature if possible. Use the highest agreed upon algorithm possible to ensure pull request message responses are encrypted.

Message Options

Enable **Reception Awareness**. Reception Awareness allows GoAnywhere to report whether a message has been successfully received or not.

Push Processing Modes

Receipt Signature

Enable **Sign Receipt**. Signed receipts help ensure nonrepudiation. Use the highest agreed upon algorithm possible. Signed receipts help ensure nonrepudiation.

Message Decryption

Use a unique key pair for each trading partner.

Message Options

Set the **Reply Mode** to 'Synchronous'. This ensure that the message receipt arrives at the correct endpoint.

Uploads

Ensure that the upload directory is pointing to an encrypted folder where files will be encrypted at rest.

Require

Set **Encryption** and **Signature** to 'Yes'. This allows GoAnywhere to throw an error if either are missing from a message.

Web User Settings

The following section provides all recommendations for the Web User Settings. Only fields and options with recommended settings will be addressed.

To manage the Web User Settings:

1. Log in as an Admin User with the **Security Officer** role. If your user account is assigned to a custom Admin User Role, your ability to view, modify, or execute actions on this page are based on the permissions specified for that role.
2. From the main menu bar, select **Users**, and then click the **Web User Settings** link.

General

Disable Inactive Web User Accounts After

Do not set this value to '0' as this disables the setting. Consult your internal security team for recommendations.

Password Policy

Set password policy parameters in accordance with company password policy. If you do not have an official security policy, our recommendations follow. Consult your internal security team for further recommendations.

NOTE:

If you use Active Directory to authenticate users, your password policy is managed by Active Directory.

Password Strength

Enforce Settings

Enforce password strength settings.

Minimum Password Length

Set the minimum password strength to 8.

Minimum Number of Upper Case Letters

Set a minimum of 1.

Minimum Number of Lower Case Letters

Set a minimum of 1.

Minimum Number of Digits

Set a minimum of 1.

Minimum Number of Special Characters

Set a minimum of 1.

Allowable Special Characters

Allow all special characters.

Password Age

Minimum Password Age

Set a Minimum Password Age to 1.

Maximum Password Age

Do not set the Maximum Password Age to zero (0). The industry standard is 90 days. Consult your internal security team for recommendations.

NOTE:

Applying a Maximum Password Age can affect automated and service level accounts that are not LDAP managed.

Password History

Enforce Password History

Enable.

User Name Policy

Set password policy parameters in accordance with company password policy. Consult your internal security team for recommendations.

NOTE:

If you use Active Directory to authenticate users, your password policy is managed by Active Directory.

Device Policy

PIN Verification Required

Enable PIN verification.

PIN Length

Set a PIN length of at least 6 digits.

Admin Approval Required

Require admin approval for all devices.

Notify Web User Device Managers

Enable so that Device Managers are notified via email when a Web User registers a device.

Notify Additional Email Addresses

Add one or more email recipients to be notified when a Web User registers a device for GoDrive and the device requires admin approval or has become activated. Separate multiple email addresses with commas.

Require Device Reauthentication

Enable.

Reauthenticate Every

Set reauthentication to every 7 days. Consult your internal security team for recommendations.

Profile

Enable the 'Unique Email Addresses' setting to allow for consolidated permissions and better traceability. Consult your internal security team for recommendations.

Anonymous

Disable 'Allow Anonymous Web User'.

Web User Self-Registration

The following section provides all recommended settings for Web User Self Registration. Only fields and options with recommended settings will be addressed.

To access the Web User Self-Registration page:

1. Log in as an Admin User with the **Security Officer** role.
2. From the main menu bar, select **Users**, and then click the **Web User Self-Registration** link.

Web User Self-Registration

Self-Registration Allowed

Disable this feature. Web User Self-Registration allows your employees and trading partners to create an account in GoAnywhere through the Web Client interface.

NOTE:

If using Certified Delivery, users will need to be manually created or sync'd with LDAP/SAML if this setting is disabled.

If your environment requires the use of Web User Self-Registration, it is recommended to ensure the following configurations are in place.

Email Pattern

Limit the email patterns allowed to self register.

Permission

Allow **only** the emails necessary to register. **Deny** all others.

Web User Template

Select a Web User Template that gives created Web Users the minimum permissions necessary to GoAnywhere.

NOTE:

When configuring the Home Directory for created Web Users, it is recommended to generate the users' home folders based upon the user.name variable. The default setting for Home Directory will use this value to create the Web Users home directory under the configured webdocs location. Using the other offered variable values is not recommended, as these values are not required to be unique within GoAnywhere. Ensure that careful consideration is given to any folder access given to a Web User, to ensure that selected variable values do not unintentionally give Web Users access to the same directory locations.

Requires Approval

Enable Requires Approval

Notify Web User Managers

Enable Notify Web User Managers

User Email as User Name

Enable Use Email as User Name

Domains

The following section provides all recommended settings for GoAnywhere Domains. Only fields and options with recommended settings will be addressed.

To manage Domains:

1. Log in as an Admin User with the **Security Officer** role.
2. From the main menu bar, select **Users**, and then click the **Domains** link.

Allow Execute Native Command

This option determines if Projects and Triggers in this Domain can use the Execute Native Command task or Execute Native Command Trigger action to run commands on the server where GoAnywhere is running. Use the principle of least privilege.

File Access Restrictions

The File Access Restrictions options determine if Web Users, Admin Users, and Resources in this Domain are restricted to specific folders. Use the principle of least privilege.

Key Management System

Allow File Based Keys

Disable file based keys whenever possible as file based keys are accessible from the file system.

Login Settings

The following section provides all recommended settings for user Login Settings. Only fields and options with recommended settings will be addressed.

To manage Login Settings:

1. Log in as an Admin User with the **Security Officer** role. If your user account is assigned to a custom Admin User Role, your ability to view, modify, or execute actions on this page are based on the permissions specified for that role.
2. From the main menu bar, select **Users**, and then click the **Login Settings** link.

Default Login Methods

Set 'GoAnywhere' as the default login method for Admin and Web Users.

Two-Factor Authentication Options

Enable two-factor authentication.

Reporting

Logs, reports, and log settings are available to authorized Admin Users from the Reporting drop-down menu.

Logs are useful for troubleshooting errors and monitoring events such as file transfers and server activity. The logs can be sorted by column, as well as exported to a CSV formatted file.

Log Settings

The following section provides all recommended settings for Log Settings. Only fields and options with recommended settings will be addressed.

To administer Logs, log in as an Admin User with the **Product Administrator** role.

From the main menu bar, point to **Reporting** and then click **Log Settings**.

General Tab

Tamper-Evident Logging

Enable Tamper-Evident Logging

NOTE:

If you have any log exemptions configured, those events will not be logged.

Security Settings Audit Report

While the Security Settings Audit report is intended to analyze your GoAnywhere product's security settings and determine if they comply with the Payment Card Industry Data Security Standards (PCI-DSS), this report is also useful in locating potential weaknesses in your GoAnywhere configuration.

For each security setting, the report will indicate if the setting meets the PCI-DSS standard using one of the following statuses:

- **Pass** - The setting meets the PCI-DSS requirement.
- **Fail** - The setting does not meet the PCI-DSS requirement. Recommended steps to correct the setting are provided.
- **Warning** - Further research is required to ensure your system meets the specified requirement. Recommended steps to correct the setting are provided.
- **Not Applicable** - A check on this setting is not required, typically due to GoAnywhere features that you are not licensed to use.
- **Fatal** - Indicates a configuration problem is preventing GoAnywhere from accessing the appropriate data.

NOTE:

Running the Security Settings Audit Report requires the Advanced Reporting Module. If you do not have access to this feature, reach out to your sales rep for temporary access.

Glossary

N

nonrepudiation

Creating a proof of the origin or delivery of data, thus preventing the recipient from falsely denying that data has been received and preventing the sender from falsely asserting that data has been sent.

P

principle of least privilege

A user should be given only those privileges needed to complete a given task. If a user does not need an access right, the user should not have that right.