

# Top 10 Tips for Securing Your FTP or SFTP Server

Presented by Linoma Software,  
a HelpSystems company.



# Introductions



**Bob Luebbe, CISSP**  
*Chief Architect*



**Steve Luebbe**  
*Director of Engineering*



**Dan Freeman, CISSP**  
*Senior Solutions  
Consultant*



# Agenda

---

- About Linoma Software
- The 3 tenets of Information Security
- A summary of regulations that govern data security
- Typical issues found in FTP/s and SFTP servers
- The Top 10 Tips to secure your FTP/s or SFTP server
- Additional considerations
- Brief discussion of the GoAnywhere Secure FTP server
- Feel free to ask questions throughout the webinar





# Linoma Software Background

- Founded in 1994—based in Nebraska
- Growing and financially stable



- Active R&D with focus on data automation and security
- Division of **helpsystems** with 10,000 customers and over 500 employees around the world
- Member of PCI Security Standards Council





# CIA—The 3 Tenets of Information Security

## **C**ONFIDENTIALITY:

*Information is not disclosed to unauthorized individuals, entities, or processes*

## **I**NTEGRITY:

*The accuracy of data is maintained and assured over its entire lifecycle*

## **A**VAILABILITY:

The system and data is available to authorized entities without disruptions





# Top Regulations for Data Security in the U.S.



**HIPAA:** Requires the protection of any communications containing PHI (Protected Health Information) which is transmitted electronically over open networks from being intercepted by anyone other than the intended recipient.



**Gramm-Leach-Bliley Act (GLBA):** Requires financial institutions to implement safeguards to protect the security, integrity, and confidentiality of customer information, no matter how it is stored or transmitted.



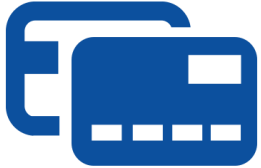
**State privacy laws:** Enacted for the protection of PII (Personally Identifiable Information). Most states have notification laws, while others are more specific on how data is protected. For instance, Massachusetts requires the encryption of any PII that is transmitted or stored.



**FISMA:** The Federal Information Security Management Act is legislation that defines a comprehensive framework to protect government information, operations, and assets against natural or man-made threats. FISMA was signed into law part of the Electronic Government Act of 2002.



# PCI DSS Security Standard



PCI DSS requires the protection of any payment card information (credit/debit card info) that is stored or transmitted.

- ▶ PCI requirements are worldwide (not focused on a specific region)
- ▶ The latest version 3.2 requires multi-factor authentication for non-console administrator access
- ▶ Standards include detailed requirements for user authentication, password strengths, network segmentation, firewalls, encryption, key management, auditing, etc.
- ▶ Many of the tips in this webinar will refer to specific requirements from the PCI DSS standards

*Even if you do not process cardholder data, the PCI DSS standards are a comprehensive security reference.*

# Data Security in Europe



## GDPR—General Data Protection Regulation

- ▶ Most important change in data privacy regulation in 20 years
- ▶ Enforcement begins on May 25, 2018
- ▶ Strengthens and unifies data protection for all individuals within the EU
- ▶ Extends to all foreign companies that process data for EU residents
- ▶ Fines can be up to €20 million or 4% of global company's revenues for the preceding financial year, whichever is the greater



Poll: Which compliance requirements are presenting the biggest challenge for your file transfers?





# Top FTP Server Issues

---

**FTP server software is not up to date**

**Software is not configured properly**

**Has too many admins with excess rights**

**Vulnerable protocols or ciphers are enabled**

**Too difficult to administer and monitor**

**Lacking alerts and detailed audit trails**



 UP NEXT...

## Top 10 Tips for Securing your FTP Server

# TIP #1

## Disable Standard FTP

### ► Disable standard FTP protocol:

1. No privacy—Transmissions are not encrypted (data, commands, users, passwords in clear text)
2. No integrity—Data can be modified in transit without knowledge
3. Poor authentication—Only has one factor of authentication (user/password)

### ► Use one of these alternatives:

#### **FTPS:** FTP over SSL/TLS

- Can also use an X.509 certificate for dual factor authentication
- Uses a control port and a series of data ports

#### **SFTP:** FTP over SSH file transfer protocol

- Can also use a SSH key for dual factor authentication
- Only one port (default 22) needs to be used
- Built into Linux and UNIX operating systems

### ► See **PCI DSS requirements 2.2.3 and 4.1**

#### From PCI DSS Requirement 2.2.3:

*"Use secured technologies such as SSH, SFTP, TLS, or IPSec to protect insecure services such as NetBIOS, file-sharing, Telnet, FTP, etc."*

## TIP #2

# Use Strong Encryption and Hashing



### Encryption ciphers are used to protect the data transmission

- ▶ Disable older encryption ciphers like Blowfish and DES
- ▶ Only use strong ciphers of AES or TDES

### Hash (MAC) algorithms are used to verify the integrity of the transmission

- ▶ Disable older hash/MAC algorithms like MD5 or SHA-1
- ▶ Use only strong hash algorithms in the SHA-2 family like SHA-256 and SHA-512

***These recommendations apply to both SFTP and FTPS servers***

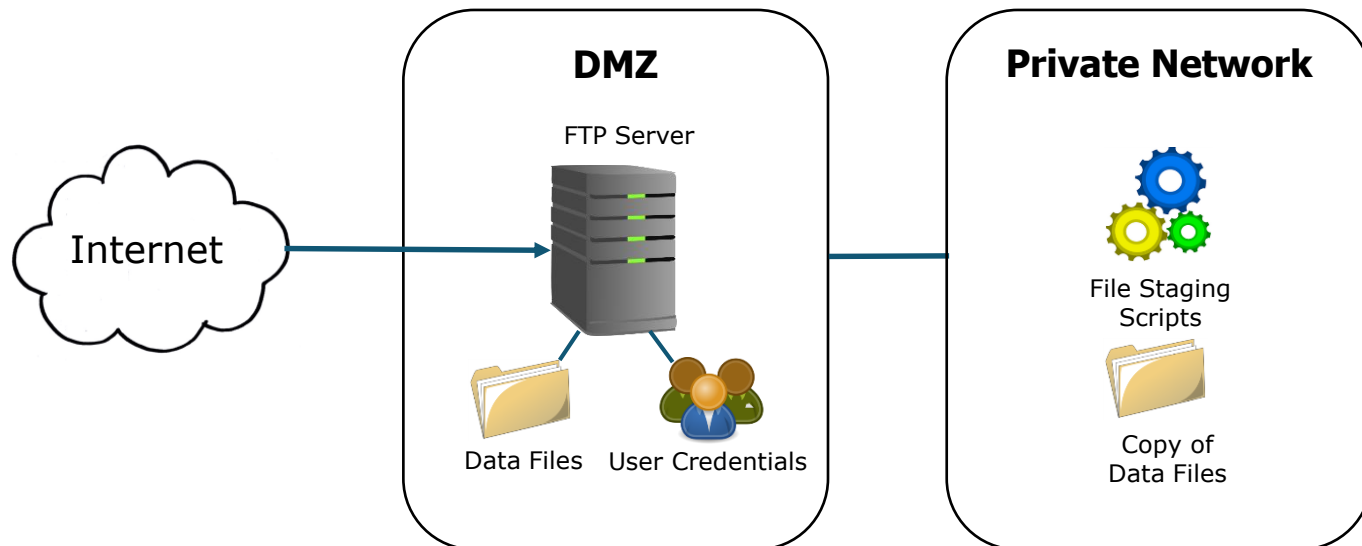
### From PCI DSS Requirement 4.1:

*"Use strong cryptography and security protocols to safeguard cardholder data during transmission over open, public networks."*



# Problems with FTP Servers in the DMZ

- The DMZ is more vulnerable to attacks since it is public facing
- Files could potentially be accessed by hackers
- User credentials are outside of the safety of the private network
- The FTP server software itself may be compromised
- Have to "stage" files between the DMZ and the Private Network

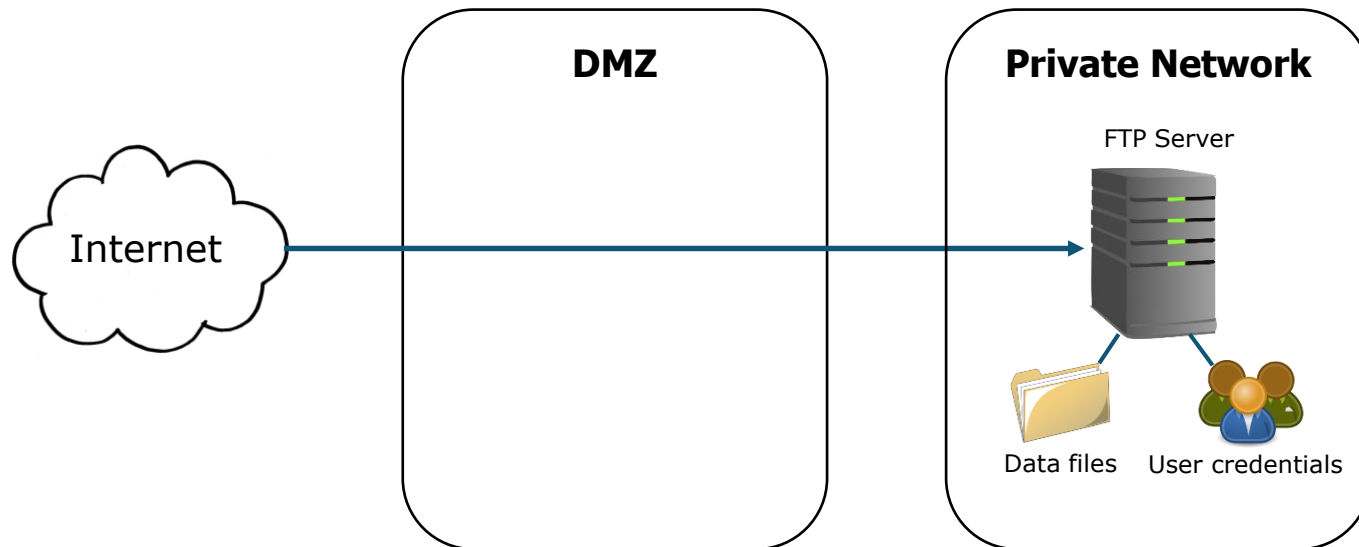




# What if Installed into the Private Network

Files and user credentials are now in the private network, which is good. However...

- You have to open inbound ports into private network
- Possible risks of a network intrusion
- May not pass an audit or meet compliance requirements



# TIP #3

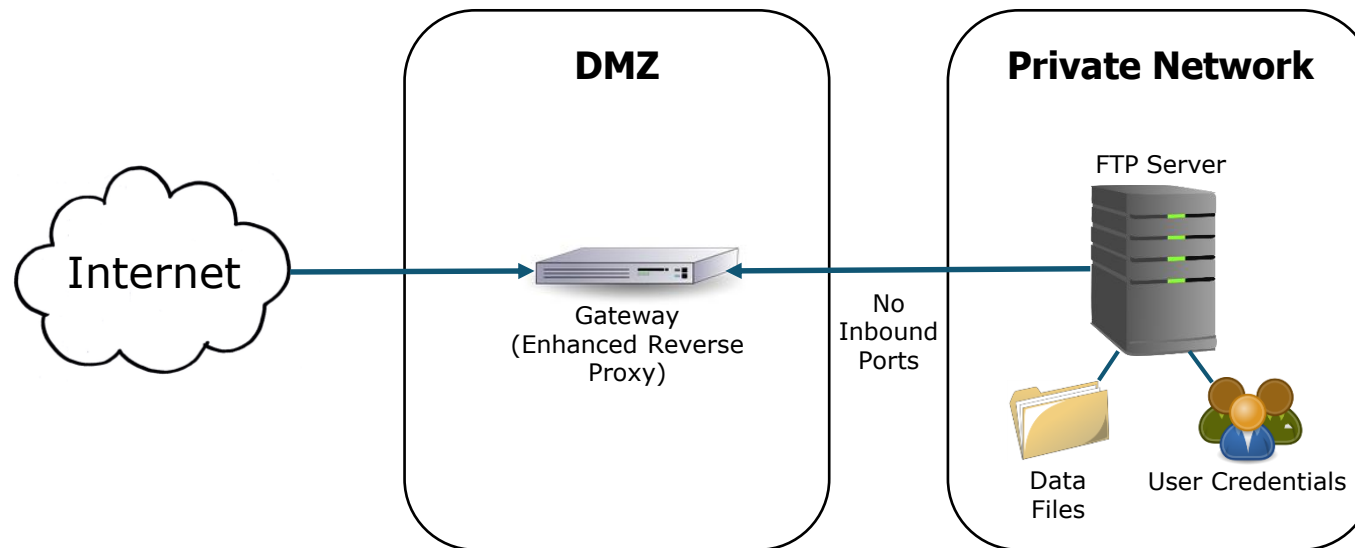
## Place Behind a Gateway



- ▶ DMZ Gateway acts as an enhanced reverse proxy
- ▶ Control channel is opened from the private network to the DMZ
- ▶ No ports are required into the private network
- ▶ Files and user credentials stay in the private network
- ▶ See PCI DSS requirement 1.2.1, 1.3.2, 1.3.6, and 1.3.7

### From PCI DSS Requirement 1.3.7:

*"Place systems components that store cardholder data in an internal network zone, segregated from the DMZ and other untrusted networks."*



## TIP #4

# Implement IP Blacklists and Whitelists



A blacklist denies a range of IP addresses that can access the system

- ▶ Predefine ranges of IP addresses to block (e.g. China, Russia)
- ▶ Set up auto-blacklisting for:
  - Denial-of-Service (DoS) attacks
  - Brute force attacks (uses combinations of invalid users/passwords)
  - Malicious user names (root\*, admin\*, etc.)
- ▶ You can either temporarily or permanently blacklist IP addresses

A whitelist allows only specified IP addresses to access the system

- ▶ May want to only allow trading partners to connect from certain IPs
- ▶ Works “ok” as long as the trading partner uses fixed IP addresses

### PCI DSS

*See requirements  
1.2.1 and 6.6*

***Blacklists and whitelists are not foolproof since IP addresses can be spoofed...***



## TIP #5

# Harden your FTPS Server



- ▶ Do not use Explicit FTPS, unless you force encryption for the authentication and data channels. Alternatively use Implicit FTPS (normally at port 990).
- ▶ FTPS uses SSL or TLS protocols to protect the transmission
  - Versions: SSL 1.0, SSL 2.0, SSL 3.0, TLS 1.0, TLS 1.1, and TLS 1.2
  - Do not use any of the SSL versions or TLS 1.0
  - Only use TLS versions 1.1 or 1.2
- ▶ Use Elliptic-Curve Diffie Hellman key exchange algorithms. Older “export” key exchange algorithms were exploited by Logjam attack.
- ▶ SSL (X.509) certificates
  - Key lengths should be 2048 or 4096 bits
  - Use a SHA2 signature algorithm (224 to 512 bits)
  - Remove expired certificates
- ▶ See [PCI DSS requirements 2.2.3, 3.6.5 and 4.1](#)

### October 2014:

*A pair of Google researchers have discovered that SSL 3.0 is no longer secure due to its vulnerability to POODLE attacks.*

### BEAST Attack:

*TLS 1.0 and earlier protocols suffer from a serious flaw: the Initialization Vector (IV) blocks that are used to mask data (plaintext) prior to encryption with a block cipher can be predicted by an active man-in-the-middle (MITM) attacker.*



Poll: What type of Secure FTP Server do you have within your organization?

## TIP #6

# Utilize Good Account Management



- ▶ Do not create OS-level user accounts for trading partners since it creates a potential pathway for attacks on that system
- ▶ User credentials should be stored separate from the FTP application such as in LDAP, AD, or a database ([PCI DSS 2.2.1](#))
- ▶ Utilize pre-defined templates to create trading partner user accounts to ensure that consistent security settings and permissions are used. This also simplifies account creation.
- ▶ Disable anonymous users ([PCI DSS 8.5](#))
- ▶ Account user names should be at least 7 characters in length
- ▶ Non-repudiation: User accounts should not be shared between partners
- ▶ Automatically disable accounts after 6 login failures ([PCI DSS 8.1.6, 8.1.7](#))
- ▶ Disable accounts after 90 days of inactivity ([PCI DSS 8.1.4](#))
- ▶ Consider self-registration (with an approval process) to streamline user provisioning



Research sponsored by the University of Michigan found more than **1 million** FTP servers are configured with anonymous access.

## TIP #7

# Have a Good Password Policy



► Password policy should require:

- Passwords should be at least 7 characters in length ([PCI DSS 8.2.3](#)), but 10 characters are recommended by some security professionals.
- Contain both numeric and alphanumeric characters ([PCI DSS 8.2.3](#))
- Contain at least one special character (e.g. !@#\$%^&\*)

<b>Bad password:</b>	<b>washington</b>
<b>Good password:</b>	<b>Wa\$h1ngt0N</b>



- Admin passwords should change every 90 days ([PCI DSS 8.2.4](#))
- Do not allow reuse of last 4 passwords ([PCI DSS 8.2.5](#))
- Make sure the user passwords are stored using strong hashing (one-way) encryption algorithms such as SHA-2 ([PCI DSS 4.1](#))

## TIP #8

# Implement Effective Folder Security



- ▶ Restrict folder permissions as needed (e.g. upload only, download only, etc.)
- ▶ Be careful about sharing folders between trading partner accounts
- ▶ Encrypt files at rest, especially if stored in the DMZ ([PCI DSS 3.4](#))
- ▶ Retain files on FTP server only as long as needed
- ▶ Set disk quotas per user the file system is not overloaded



## TIP #9

# Lock Down Administration



- ▶ Authenticate admins against an existing AD or LDAP directory (so you don't have to store admin passwords in the FTP server)
- ▶ Do not allow remote admin access through the public internet (unless over a VPN)
- ▶ Require two-factor authentication (e.g. password and a token) for administration ([PCI DSS 8.3](#))
- ▶ Do not use default admin accounts like root or admin ([PCI DSS 2.1](#))
- ▶ Implement separation of duties. Restrict admin duties to a limited number of users ([PCI DSS 7.1](#))
- ▶ Disable inactive administrator accounts ([PCI DSS 8.1.4](#))



## TIP #10

## Follow these best practices



- ▶ Keep the FTP/s or SFTP server software up-to-date. Security patches should be applied within 30 days ([PCI DSS 6.2](#))
- ▶ If working with U.S. government data, use only FIPS 140-2 validated encryption ciphers
- ▶ For SFTP, do not use the default software version that is shown when you first log in ([PCI 2.1](#))

"Welcome to BrandX SFTP Server version 2.4"

This is a bad example of a welcome message since it gives a hacker a clue on how to potentially exploit the server.



- ▶ Keep any backend databases on a different server ([PCI DSS 2.2.1](#))
- ▶ Require re-authentication of sessions that have been inactive for 15 minutes ([PCI DSS 8.1.8](#))
- ▶ Implement good key management ([PCI DSS 3.6](#)) with a limited number of key managers ([PCI DSS 3.5.1](#))
- ▶ Periodically run vulnerability scans and penetration tests ([PCI DSS 11.3](#))



 UP NEXT...

## Other Considerations for your SFTP or FTPS Server



# Send Alerts on Warnings & Errors

---

- Send instant warning/error alerts via email or text messages
- Feed alerts into a central SYSLOG monitoring system
- Potential alerts:
  - When a user login fails
  - When an upload or download fails
  - When an IP address is blacklisted due to an attack
  - Other security-related events
- Sample alert:

```
Alert message: User Account Disabled.  
User account: TestUser  
IP address:    139.224.23.1  
Date/time:    March 14th, 2017 14:32:32  
Reason:       More than 5 failed login attempts
```





# Generate Detailed Audit Trails

- Audit all activity on the FTP/s or SFTP server ([PCI DSS 10.0](#))
- Logs should be easy to filter and report by user, date, time, IP, etc.
- Example:

Date / Time	Command	IP Address	User	File	Remarks
3/14/17 7:46:00	Login	209.191.2.3	partnerabc		
3/14/17 7:47:12	Download	209.191.2.3	partnerabc	orders1.csv	
3/14/17 7:47:14	Download	209.191.2.3	partnerabc	orders2.csv	
3/14/17 7:48:16	Upload	209.191.2.3	partnerabc	confirmation.xml	
3/14/17 7:49:18	Logout	209.191.2.3	partnerabc		
3/15/17 3:23:00	Login - Failed	171.8.79.143	root		Malicious user name
3/16/17 0:13:21	Login - Failed	139.224.24.26	admin		5 invalid login attempts
3/17/17 9:05:43	Login - Failed	125.88.74.122	test		Invalid user id

- Audit log retention:

PCI DSS: 1 year

SOX: 7 years

FISMA: 3 years

HIPAA: 6 years

GLBA: 6 years

- Recommended to also audit all administrator activity on the server



# Consolidate SFTP and FTPS Servers

- ▶ Don't use a different SFTP or FTPS server for each department – Use domains instead!
- ▶ A domain is like a “security zone” with its own administrators, trading partner accounts, authorized folders and audit logs
- ▶ Shares a common set of global configurations and security settings
- ▶ Simplifies upgrades and overall maintenance of the software
- ▶ Ensures consistency in security and simplifies audits

## SFTP or FTPS Server

### Marketing Domain



Admins



Trading  
Partners



Folders



Logs

### HR Domain



Admins



Trading  
Partners



Folders

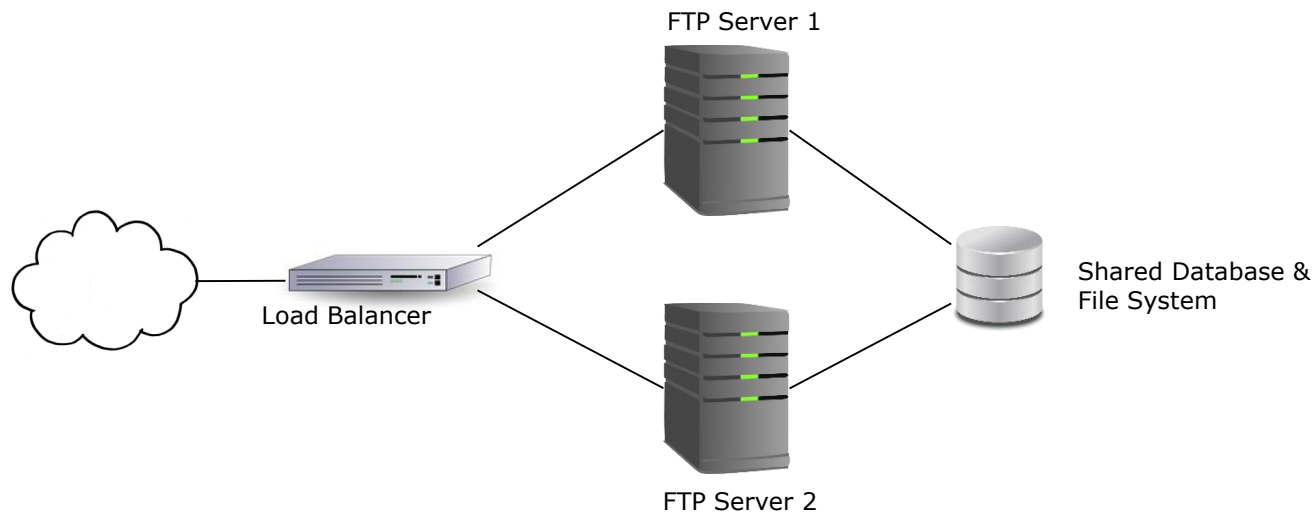


Logs



# Set up Clustering for High Availability

- Clustering allows you to have two or more servers working in parallel
- Provides for high availability (active-active), which is one of the key tenets of Information Security
- Provides Load Balancing—Distributes the workload over multiple servers
- Need to use a shared database and file system





# Summary of Tips

- Disable the Standard FTP protocol – Use SFTP or FTPS instead
- Use strong encryption and hashing algorithms like AES, TDES and SHA-2
- Place your FTP servers behind a DMZ Gateway
- Implement IP Blacklists and Whitelists
- Harden your FTPS server (e.g. only use TLS versions 1.1 or 1.2)
- Utilize good user management methods (e.g. use templates to create Partner accounts)
- Have a good password policy
- Implement effective folder and file security
- Lock down administration of your FTP server
- Send alerts on warnings and alerts
- Generate detailed audit trails
- Consolidate multiple FTP Servers
- Set up Clustering for high availability



Poll: What is the biggest challenge with your SFTP or FTP/s Server?



 UP NEXT...

## Introduction to the GoAnywhere MFT solution

# GoAnywhere® Managed File Transfer



## Access Anywhere



Web Browser,  
Command Line, API...

- Workflow Automation
- Encryption
- Data Translation
- Scheduler
- Folder Monitors
- Inbound Services
- Ad Hoc and Batch
- Secure Forms
- Secure Email
- Partner Management



**GO ANYWHERE®**  
Managed File Transfer

## Alerts



## Audit Logs & Reports



## FTP



SFTP, SCP, FTPS, FTP

## File Systems



Windows, Linux, Unix,  
AIX, IFS, Solaris, UNC,  
Amazon S3, WebDAV...

## Web Servers



AS2, HTTP, HTTPS,  
Web Services,  
SOAP, REST

## Databases



SQL Server, MySQL,  
DB2, Oracle, PostgreSQL,  
Sybase, Informix...

## Applications



Scripts, Programs,  
Commands, MQ, SNMP

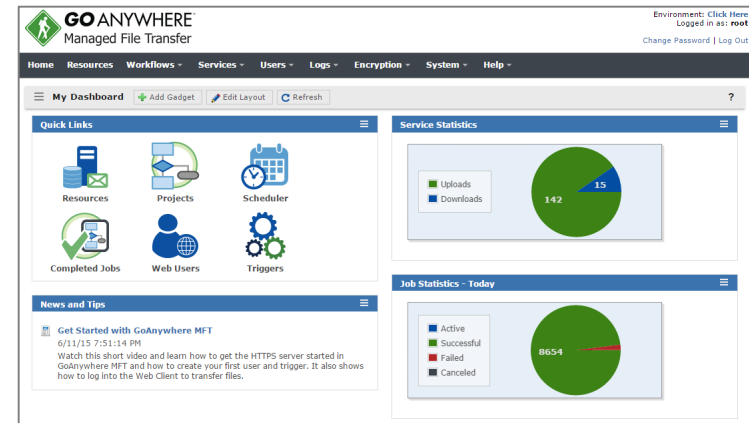
## Email and SMS



SMTP, POP3, IMAP,  
SMS (text messages)

# GoAnywhere Enterprise-level Features (1 of 2)

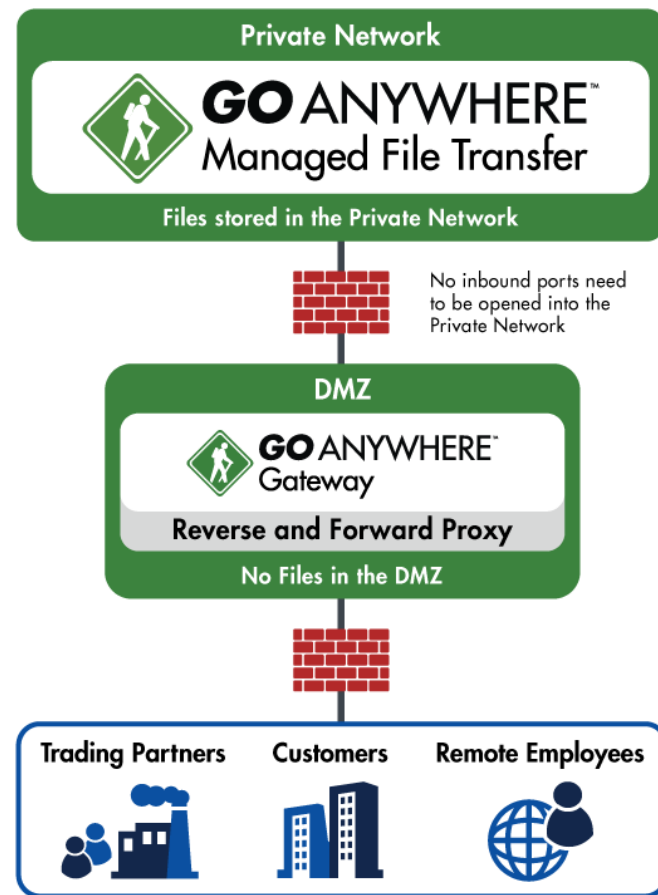
- **Multi-platform:** Installs to most operating systems including IBM i, Windows, Linux, AIX, UNIX, Amazon, and Azure.
- **Batch and Ad Hoc:** Allows organizations to perform both scheduled batch transfers and user-to-user file sharing.
- **Auditing:** Generates detailed audit logs of all file activity including batch, ad hoc, inbound, and outbound transfers.
- **Interface:** Provides a browser-based interface for all administration and monitoring. No desktop client is needed.
- **Inbound Services:** Allows inbound connections from trading partners over SFTP, FTP/S, HTTPS, and AS2 (Drummond Certified).
- **Encryption:** Protects files "at rest" and "in-motion" with FIPS 140-2 validated AES-256 encryption.
- **Key Management:** Provides integrated tools for creating and managing OpenPGP keys, SSH keys, and SSL certificates.
- **Admin Controls:** Implements role-based administration, security domains, and granular permission controls.





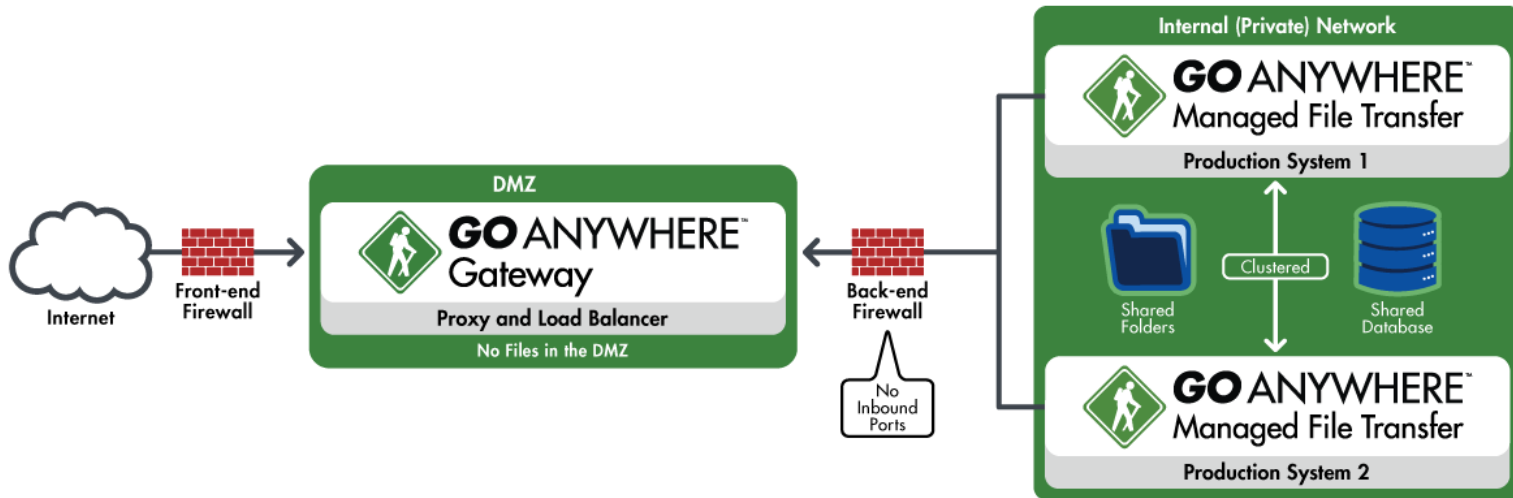
# GoAnywhere Enterprise-level Features (2 of 2)

- **Private Cloud:** Eliminates the need for public file sharing services like Dropbox, Box, Google Drive, and OneDrive.
- **Customer Portal:** Allows you to provide custom-branded web interfaces for secure file transfers over HTTPS.
- **Secure Mail:** Allows employees to send large or confidential files through secure email links. Includes an Outlook plugin.
- **Two-Factor:** Authenticates with user credentials and SAML, RSA SecurID, RADIUS, SSH keys, or X.509 certificates.
- **DMZ Gateway:** Keeps services and files in the private network (out of the DMZ) without requiring inbound ports.
- **Job Control:** Provides extensive job management features including job queues and run priorities.
- **File Transfer Acceleration:** Enables high speed transmission of large files between systems using UDP channels.
- **Clustering:** Provides high availability and load balancing by connecting two or more instances together in a cluster.





# GoAnywhere Clustering



- Two or more installations of GoAnywhere MFT can be in a cluster
- GoAnywhere Gateway can load balance inbound connections
- Project workloads are distributed 'horizontally' across multiple systems
- Active-Active = Better high availability for mission-critical environments
- All systems can be managed from a central interface
- No third-party tools or software are needed



# GoAnywhere Security Features

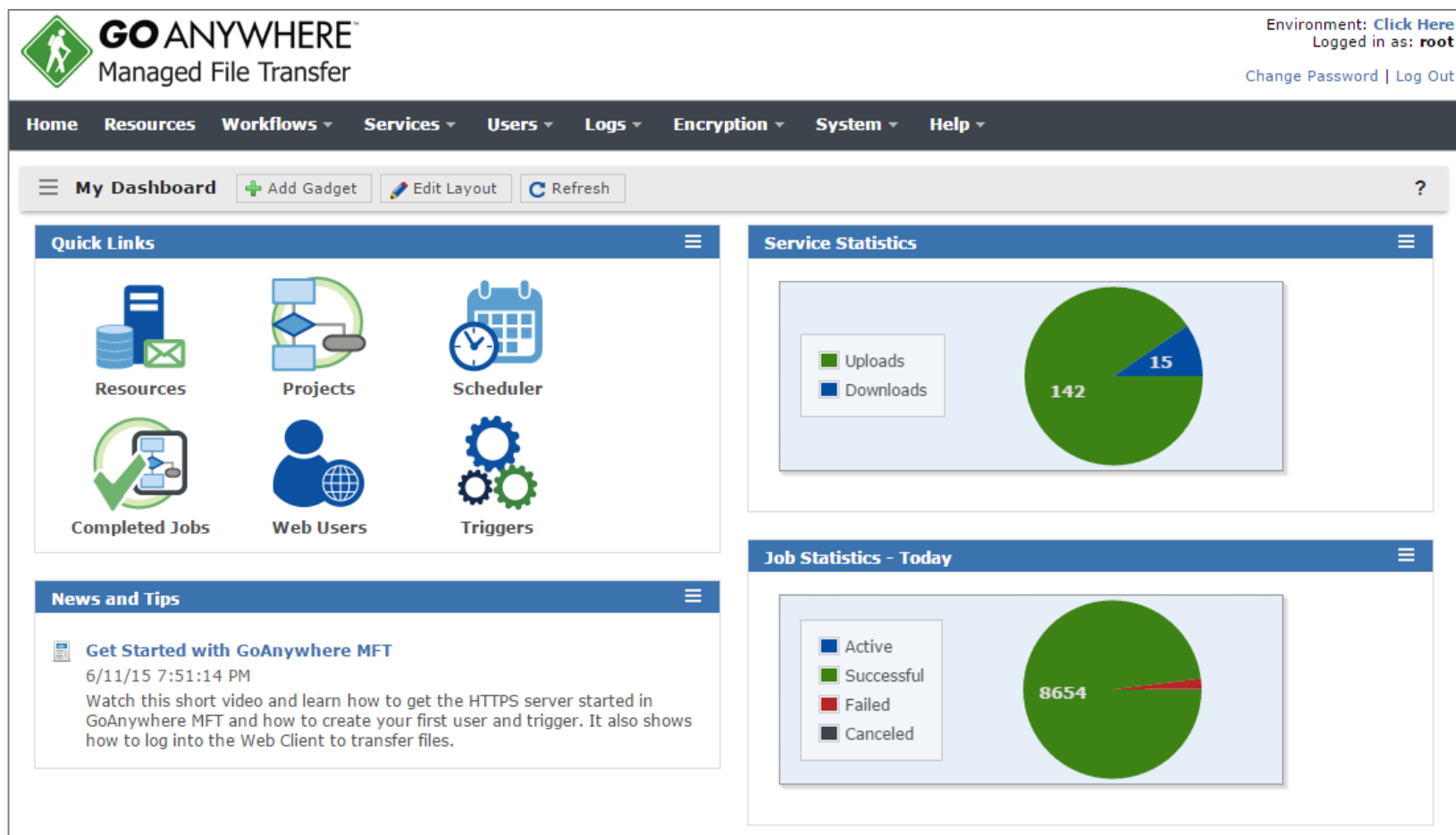
- Secure Protocols
  - SFTP: FTP over SSH
  - FTPS: FTP over SSL/TLS
  - SCP: Secure Copy
  - HTTPS: HTTP over SSL
  - Open PGP/GPG
  - ZIP with password protection
  - Encrypted email (SMIME)
  - AS2
- AES encryption (key lengths of 128, 192, 256)—NIST standard
- SSL protected console
- Helps meet compliance for PCI DSS, HIPAA, FIPS 140-2, Sarbanes Oxley, GLBA, and State Privacy Laws





# GoAnywhere Administrator

- Browser-based Dashboard
- Intelligent Gadgets
- Drag-and-Drop
- Latest HTML5 Technology





# GoAnywhere Trading Partner Management

- Create trading partner accounts using Templates, APIs, batch load or self-registration
- Authenticate users against AD, LDAP, IBM i, RADIUS, RSA SecurID or database.
- SAML for Single Sign-on
- Grant individual permissions or adopt permissions from groups
- Restrict to FTP, SFTP, FTPS, HTTP/s, AS2
- Restrict access to certain folders and permissions (e.g. upload, download, delete, rename, etc.)
- Restrict to certain IPs
- Set time limits

**Edit Web User**   ?

**General** | Authentication | Groups | Features | Folders | IP Filter | Time Limits | AS2

User Name:

Enabled: ☒

First Name:

Last Name:

Description:

512 Characters Remaining

Organization:

Email Address:

Phone:



# GoAnywhere Web Client for Ad-Hoc File Transfers

- Provides your trading partners with secure browser-based access to your system for uploading and downloading files
- Rebrand with your company logo and privacy policy
- Full audit trails and event triggers

The screenshot displays the GoAnywhere Web Client interface. At the top, the logo and "Web Client" text are on the left, and the user status "Logged in as: kharris" and "Last Login: 6/18/15 6:09:18 AM" are on the right. Below this is a navigation bar with links: Dashboard, GoDrive, Secure Mail, Secure Folders, My Account, Activity Report, and Invite Users. The main content area is titled "Secure Folders" and shows a "Location" field set to "/". Below the location field is a table of files. The first two files, "Corporate\_Overview.pdf" and "Customer\_List.pdf", are selected, indicated by blue checkmarks in the selection column. The table has columns for Name, Date Modified, and Size. At the bottom of the interface, it shows "2 Rows Selected" and buttons for "Delete", "Send To", "Download", and "Copy to GoDrive".

	Name	Date Modified	Size
<input checked="" type="checkbox"/>	Corporate_Overview.pdf	6/18/15 6:11:49 AM	390.02 KB
<input checked="" type="checkbox"/>	Customer_List.pdf	6/18/15 6:11:52 AM	252.73 KB
<input type="checkbox"/>	GoAnywhere-on-Automatic.jpg	6/18/15 6:11:53 AM	167.60 KB
<input type="checkbox"/>	GoAnywhere_Customer_Care_Guide.pdf	6/18/15 6:11:54 AM	545.09 KB
<input type="checkbox"/>	GoAnywhere_UC_case_study.pdf	6/18/15 6:11:55 AM	955.49 KB
<input type="checkbox"/>	High_Availability_Diagram.pdf	6/18/15 6:11:55 AM	48.78 KB



# GoAnywhere Audit Logs

- Audit logs are stored for every transaction (login, upload, download, rename, etc.) for all services
- Search using a wide variety of filter criteria
- View online or export to CSV
- Can optionally feed to a SYSLOG server
- Also stores audit trails for admin activity

GoDrive Log

Basic Search

Advanced Search

Date Range \*

Jun 18, 2015 00:00

to \*

Jun 19, 2015 00:00

User

Success

Event Type

Event ID

Local IP

Remote IP

Session ID

File Name

System Name

Search

	Start Time	Event Type	Success	File Name	Folder Name	User
Q	6/18/15 6:12:11 AM	File Downloaded	✓	Solution_Requirements.pdf		kharris
Q	6/18/15 6:12:10 AM	File Downloaded	✓	Secure_Network_Diagram.docx		kharris
Q	6/18/15 6:12:07 AM	File Downloaded	✓	Processing XML Files.pdf		kharris
Q	6/18/15 6:12:05 AM	File Downloaded	✓	PHI_Requirements.pdf		kharris
Q	6/18/15 6:12:01 AM	File Downloaded	✓	Medical_Cost_Savings.xlsx		kharris
Q	6/18/15 6:11:56 AM	File Downloaded	✓	HIPAA_Compliance.pdf		kharris
Q	6/18/15 6:11:55 AM	File Downloaded	✓	High_Availability_Diagram.pdf		kharris
Q	6/18/15 6:11:54 AM	File Downloaded	✓	GoAnywhere_UC_case_study.pdf		kharris
Q	6/18/15 6:11:54 AM	File Downloaded	✓	GoAnywhere_Customer_Care_Guide.pdf		kharris
Q	6/18/15 6:11:53 AM	File Downloaded	✓	GoAnywhere-on-Automatic.jpg		kharris

Showing 1 - 10 of 36

1

2

3

4

>>

Rows 10

Export Page

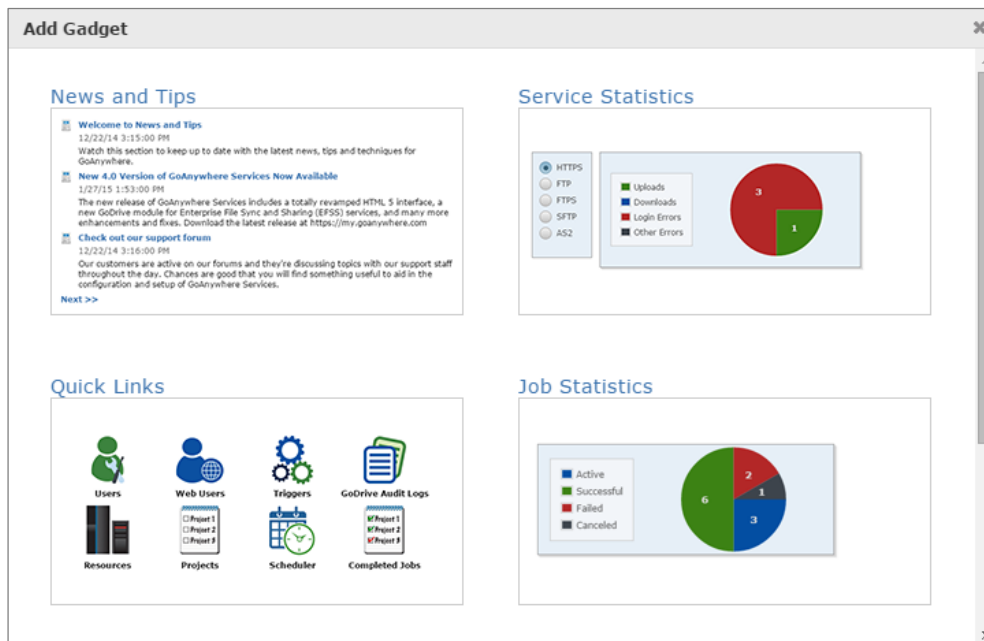
Export Results

Columns



# GoAnywhere Enterprise Dashboards

- Users can customize the dashboard with 23 unique gadgets
- Choose which icons, statistics, and reports to view
- Dashboards can be shared with other users
- Includes a 'Dashboard Manager' role to create and manage dashboards for others





# GoAnywhere Reports Available

- **Admin User Activity Details** - Displays all admin activity for the selected components
- **Blacklisted IP Addresses** - Displays blocked IP addresses and their creation timestamp
- **Completed Jobs Detail** - Displays completed jobs, status and the user who ran the job
- **Completed Jobs by Project** - Displays completed job details based on their projects and the specified date range
- **Completed Jobs Statistics** - Displays the total number of jobs processed during a specified date range
- **Database Statistics** - Displays the number of rows for each database table in GoAnywhere MFT
- **Expiring Open PGP Keys** - Displays any Open PGP keys that will expire within a specified date range
- **Expiring SSL Certificates** - Displays SSL Certificates that will expire within a specified date range
- **File Transfer Summary** - Displays the total number of files transferred during the specified date range
- **Global Activity Details** - Displays all activity for the selected features based on the search term provided
- **GoDrive Disk Usage** - Displays the total amount of disk usage for each GoDrive user
- **Job Count Summary** - Displays a pie chart of the number of jobs processed within a specified date range
- **Secure Mail Activity** - Displays Secure Mail audit activity
- **Secure Mail Disk Usage** - Displays the Secure Mail disk usage for each Web User sorted by size
- **Secure Mail Package Sizes** - Displays a list of Secure Mail Packages and their sizes
- **Security Settings Audit** - Displays critical security settings for PCI DSS standards compliance
- **Service Activity by Module** - Displays all activity for inbound services within the specified date range
- **Service Activity Summary** - Displays the number of uploads and downloads for selected protocols
- **Service Errors** - Displays all errors for the selected inbound services within the specified date range
- **Trigger Activity** - Displays executed Triggers, status and associated event types
- **Unresolved Jobs** - Displays Jobs that failed during a specified date range that have not yet been resolved
- **Web User Logins** - Displays a list of user logins for the time period specified
- **Web User Transfer Count Activity** - Displays the number of file transfers performed by user
- **Web User Transfer Size Activity** - Displays the total size of transferred files by each user

***You can also create custom PDF reports from the audit database***



# GoAnywhere Report Example

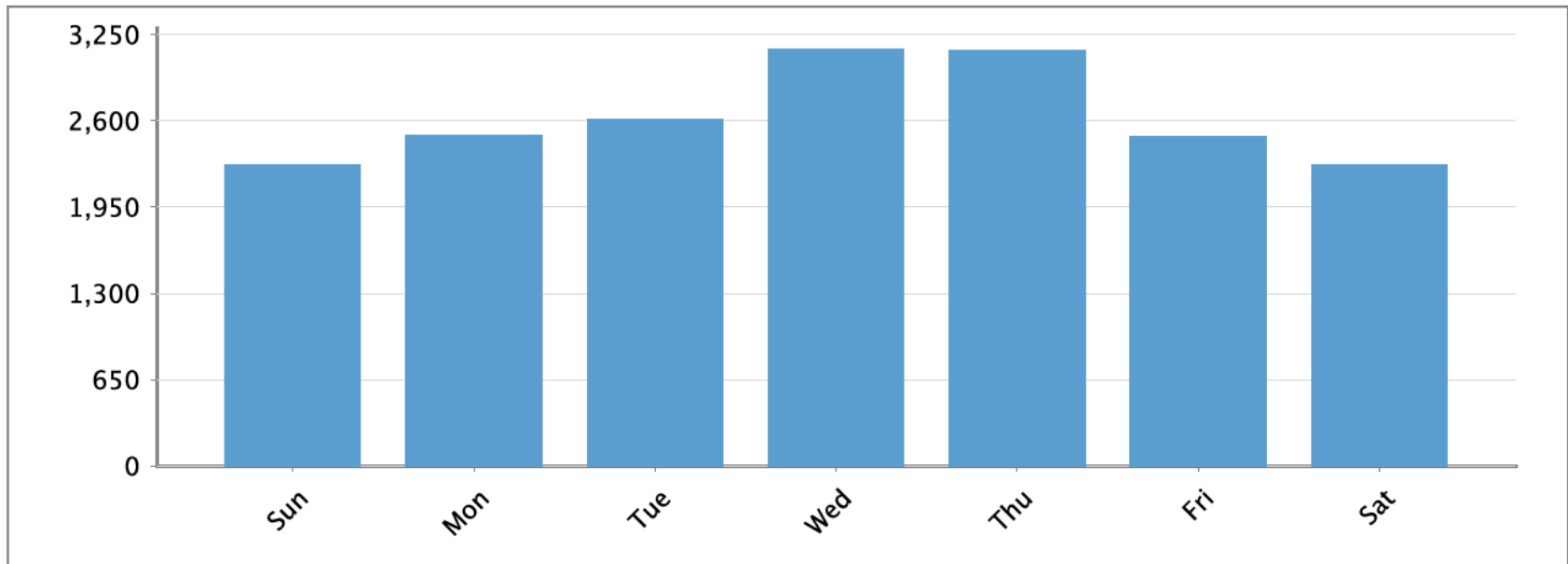


## File Transfer Summary



**GO ANYWHERE®**  
Managed File Transfer

Generated On 3/23/17 11:16:44 AM  
Date Range 2/22/17 12:00:00 AM to 3/24/17 12:00:00 AM  
Grouped By Day of Week  
Modules Secure Folders, SFTP  
Transfers 18389



# GoAnywhere Security Settings Audit Report




- Analyzes 75 security settings in GoAnywhere to determine how they comply with the PCI DSS standards.
- For each security setting, the report will indicate if the setting meets the standard with one of these statuses:

**Pass** The setting meets the PCI DSS requirement

**Fail** The setting does not meet the PCI DSS requirement.

**Warning** Further research is required to ensure your system meets the specified requirement.

- If a Fail or Warning, a recommendation is provided on how to correct the issue

Security Settings Audit			
			
Generated On	3/23/17 10:36:30 AM		
Organization	Linoma Software - All		
Environment	Linoma Software - Demo		
Passed	47		
Warning	2		
Failed	26		
Fatal	0		
Not Applicable	0		
Security Check	Status	Recommendation	PCI DSS Section
GoAnywhere Gateway is enabled to provide a reverse proxy service for inbound connections.	Passed		1.2.1, 1.3.2, 1.3.6, 1.3.7
The default Admin User 'administrator' is disabled or is not using the default password.	Passed		2.1
The default Admin User 'root' is disabled or is not using the default password.	Passed		2.1
The default SSL certificate is not used by the HTTPS admin server.	Passed		2.1
The default SSL certificate is not used by the HTTPS/AS2 service.	Passed		2.1
The default SSL certificate is not used by the FTP service.	Passed		2.1
The default SSL certificate is not used by the FTPS service.	Passed		2.1
The default SSH host keys are not used by the SFTP service.	Passed		2.1
The SFTP service software version, which is shown after user login, does not contain the default string of "GoAnywhere".	Failed	The Software Version for the SFTP service is not specified. Within the Service Manager, specify a value for the Software Version for the SFTP service to show after login. The Software Version should not be left blank or show the word "GoAnywhere".	2.1
GoAnywhere application is separate from the database server.	Passed		2.2.1



# GoAnywhere Installation Requirements

## Linux (32-bit and 64-bit):

- |                 |   |
|-----------------|---|
| - Distributions | Red Hat, SUSE, Ubuntu, CentOS (not inclusive) |
| - Disk space    | 375 MB per product (not including user data)  |
| - Memory        | 512 MB minimum per product                    |

## Windows (32-bit and 64-bit):

- |                    |  |
|--------------------|--|
| - Operating System | Windows 2016, 2012 R2, 2008 R2, 2003, 2000, XP, Vista, 7, 10 |
| - Disk space       | 375 MB per product (not including user data)                 |
| - Memory           | 512 MB minimum per product                                   |

## IBM i (iSeries):

- |                           |  |
|---------------------------|--|
| - Operating System        | V7R1 or higher                               |
| - Disk space requirements | 275 MB per product (not including user data) |
| - Memory requirements     | 512 MB minimum per product                   |
| - JRE                     | 1.7 or later                                 |

## UNIX / AIX / Solaris / HP-UX:

- |                           |  |
|---------------------------|--|
| - Disk space requirements | 250 MB per product (not including user data) |
| - Memory requirements     | 512 MB minimum per product                   |
| - JRE                     | 1.7 or later                                 |

## Virtualized Environments:



Microsoft  
Hyper-V



**EC2**



Microsoft Azure

# Contact Information

---



**Website:** [www.goanywhere.com](http://www.goanywhere.com)  
**E-mail:** [LinomaSales@helpsystems.com](mailto:LinomaSales@helpsystems.com)

**Toll-free:** 1-800-949-4696  
**Direct:** (402) 944-4242  
**Fax:** (402) 944-4243

***Final note: Make sure to download these presentation slides in the control panel***