Shift4 Command Center Requirements

To ensure the Universal Transaction Gateways® (UTG®) is installed, configured, and operating in a secure manner and environment that is compliant with PCI DSS standards, you must read the following documents:

- *UTG PA-DSS Implementation Guide*
- The latest version of the PCI DSS documentation at www.pcisecuritystandards.org

Warning! For security implementation and best practices, see the *UTG PA-DSS Implementation Guide*.

Use of a Payment Application Data Security Standard (PA-DSS) compliant application by itself does not make an entity PCI DSS compliant, since that application must be implemented into a PCI DSS compliant environment and according to the PA-DSS Implementation Guide provided by the payment application vendor.

All applications that store, process, or transmit cardholder data are in scope for an entity's PCI DSS assessment, including applications that have been validated to PA-DSS. The PCI DSS assessment should verify the PA-DSS validated payment application is properly configured and securely implemented per PCI DSS requirements and the vendor's PA-DSS Implementation Guide. If the payment application has undergone any customization, a more in-depth review will be required during the PCI DSS assessment, as the application may no longer be representative of the version that was validated to PA-DSS.

The PA-DSS requirements are derived from the *PCI DSS Requirements and Security Assessment Procedures*. The PA-DSS details the requirements a payment application must meet in order to facilitate a customer's PCI DSS compliance. As security threats are constantly evolving, applications that are no longer supported by the vendor (e.g., identified by the vendor as "end of life") may not offer the same level of security as supported versions.

System Specifications

To ensure a smooth installation process, the system should meet the following minimum requirements:

- Processor equal to Intel Pentium 4.1, Intel Celeron, AMD Athlon, or newer
- Minimum 800 MHz processor speed
- Minimum 8 Gigabytes RAM
- Minimum 4 CPU cores
- Minimum 40 Gigabytes Hard Drive
- Minimum 10/100 Megabit Network Interface Card
- Shift4-supported Windows operating system with appropriate service packs and security updates. (See the bulleted list below for supported versions of Windows.)
- Static internal IP address per UTG
- .NET Framework 4.6.2**
- Minimum 5 Mbps download network speed per simultaneous install of UTGs using Shift4 Command Center, recommend 10 Mbps

Higher volume merchants may require a more powerful system.

**If using a Shift4 Command Center Agent that is running 2.0.1000 or higher, having .NET Framework 4.6.2 installed prior to the Shift4 Command Center installation process is no longer required because the applicable .NET Framework will be included.

Windows Firewall

Shift4 conforms to the strictest security requirements. For security reasons, the UTG must be installed on a machine behind a firewall. However, because a firewall restricts communication between your computer and the internet, it is necessary to adjust the settings for the UTG so it can communicate through the Windows firewall. Listing the UTG as an exception will accomplish the task. If the UTG is not listed, you will need to add them to the exception list.

Supported Windows Operating Systems

Note: UTG will work in a 64-bit or 32-bit environment. UTG can also operate in a virtualized environment.

- Microsoft® Windows 11
- Microsoft® Windows 10
- Microsoft® Windows 2019 Server
- Microsoft® Windows 2016 Server
- Microsoft® Windows 2012 Server
- Microsoft® Windows 8
- Microsoft® Windows 2008 Server
- Microsoft® Windows 7

WARNING! Unless used with *True* P2PE™, installing the UTG on a non-supported operating system is a violation of PCI DSS Requirement 6.2 and may also render your systems more vulnerable to a security breach.

Tip: To stay fully compliant with security standards, as well as ensure machine stability while running the UTG, make sure you keep the machine up to date with the latest Windows updates.

Internet Connectivity Requirements

For security reasons, an internal static IP address is required on every machine with the UTG installed. In addition, because of Card Association Security Requirements, the UTG must be installed on a machine that is protected behind a firewall. It is the merchant's responsibility to configure static IP addresses or networks.

Note: If you are in a DHCP environment, you can reserve an IP address to make it appear static.

Connecting to Shift4's data center requires outbound connections to TCP/IP ports 26880 and 26881. Configure the firewall for a pool of established, resultant, server, or ephemeral traffic across these ports to successfully connect. The exact name for the ephemeral type of resultant connection depends on the firewall's naming conventions. Specifically defined inbound connectivity policies are not required.

WARNING! If you have multiple internet connections, you need to have a way to switch between connections. UTG does not automatically switch to an alternate internet connection.

WARNING! The term SSL should be interpreted as the newest version of TLS. In accordance with the PCI Data Security Standard, all versions of SSL and TLSv1.0 are no longer considered "strong encryption" and should never be used for non-console access to card data environments through public networks or to transport card data over public networks. Shift4 offers the option to use SSL and TLSv1.0 due to system incompatibility issues with legacy PMS/POS systems, but it should only be considered a temporary fix. If SSL or TLSv1.0 must be used, it should only be used inside protected, non-public networks. For additional information, see Shift4's security corner.

Shift4 Command Center Communication

Shift4 Command Center is hosted on AWS.

The remote agent that sits next to the UTG needs outbound access to the following endpoints via 443:

- https://myportal.shift4.com/
- https://in4m.4tresspos.com/
- https://apigateway.s4ccprod.com/
- https://coreapi.4tresspos.com/
- https://in4mapi.4tresspos.com/
- https://s4-myportal.s3.amazonaws.com/
- https://wwimdmwghg.execute-api.us-west-2.amazonaws.com/s4
    - Hosted on AWS API Gateway.
    - The IP address range can unexpectedly change since it goes through CloudFront. (Please see https://ip-ranges.amazonaws.com/ip-ranges.json if needed.)
- https://a1-commandcenter.s3.us-west-2.amazonaws.com/
- https://shift4-cc-public-prod.s3.us-west-2.amazonaws.com/
- If FQDN is not possible, then an ANY is needed for the agent.exe to reach out.

Note: Port 18028 is used by the agent.exe to communicate to the UTG2 over the TCP socket within the same computer or server.

Note: The following are hosted on AWS S3:

- https://s4-myportal.s3.amazonaws.com/
- https://a1-commandcenter.s3.us-west-2.amazonaws.com/
- https://shift4-cc-public-prod.s3.us-west-2.amazonaws.com/

.NET Framework Requirements

For Command Center UTG installations, the .NET framework version on the target machine must be 4.6.2 or higher**.
**If using a Shift4 Command Center Agent that is running 2.0.1000 or higher, having .NET Framework 4.6.2 installed prior to the Shift4 Command Center installation process is no longer required because the applicable .NET Framework will be included.

Shift4 IP Addresses, Ports, and DNS Names

it is important to add all of our current IP address ranges to your list of trusted endpoints so that you can get the most out of our fast, secure, reliable payment processing. If you don't, you will limit the number of routes available to direct transactions, which may result in suboptimal transaction times and potential interruptions for your business.

Requirement: The following information may require action on your part, but there will be no immediate impact to your ability to process transactions. If you have IT staff, please forward this message to them and ask them to make the updates. If you do not have in-house IT support, you should contact whoever configured your company's network and ask them if they are restricting (white-labeling) any traffic through your company firewall. These features are typically only enabled in professional implementations, so if you configured your network on your own using default settings, you likely will not experience any impact from these Shift4 updates.

IP Address Ranges

At our two data center locations, there are the following IP address ranges. They run products like Lighthouse Transaction Manager (LTM), including connecting to LTM via direct server-to-server post; Shift4 Command Center; i4Go®; 4Word®; IT'S YOUR CARD® (IYC); 4Res®; as well as act as endpoints for any customer UTGs.
Add the following IP address ranges to your firewall's list of trusted endpoints:

Location/Site ID	ISP	IP Address Range	IP Address Start	IP Address Finish
Austin, Texas (A1)	Cogent	38.67.17.0/26	38.67.17.1	38.67.17.62
Austin, Texas (A1)	CyrusOne	209.172.201.0/26	209.172.201.1	209.172.201.62
Las Vegas, Nevada (S7)	Switch Communications†	66.209.76.192/26	66.209.76.193	66.209.76.254
Las Vegas, Nevada (S7)	Switch Communications†	66.209.75.128/26	66.209.75.129	66.209.75.190
Las Vegas, Nevada (S7)	Multi-BGP	104.153.8.0/21	104.153.8.1	104.153.15.254
Sterling, Virginia (VA)	Multi-BGP	104.153.8.0/21	104.153.8.1	104.153.15.254

†Switch Communications provides a blend of internet from up to 17 different carriers for redundancy.

Ports: Outbound Communication from Merchant to Shift4

Product	TCP 80, 443 (HTTP, HTTPS)	TCP 26880, 26881 (Shift4 UTG Ports)
UTG		Outbound
LTM	Outbound	
i4Go	Outbound	
4Res	Outbound	
IYC	Outbound	
4Word	Outbound	

Note: As long as TCP 80, 443, 26880, and 26881 are opened up to all four of the above ranges for outbound communication, you will be able to process successfully and will be able to continue to process in the event that Shift4 uses IP addresses in the ranges for expansion.
For additional information on specific product requirements, see the applicable documentation.

Port: Inbound Communication from Shift4 to Merchant

Product	TCP 443 (HTTPS)
4Res	Inbound

Requirement: If you are using 4Res in which our 4Res system reaches out to a server you control, HTTPS TCP port 443 must be open for inbound communication to your location. For additional information, see the *4Res Administrator Implementation Guide*.

Internet Domains for Web Browsers Accessing Shift4 Websites

In very security-conscious environments, browsing is allowed only to specific domains. If this applies to your environment, make sure your computers allow outbound communications to TCP port 80 (HTTP), TCP port 443 (HTTPS), port 26880, port 26881, and any host in the following DNS names:

- *.shift4.com
- *.lh.shift4.com‡
- *.dollarsonthenet.net
- *.shift4api.net
- *.4res.net
- *.privatelabelcard.com
- *.i4go.com
- *.4tresspos.com
- *.assets.shift4.com§

In addition, if you are using SkyTab and PAX A930 devices, make sure your computers allow outbound communications to ports 443 and 9080 and any host in the DNS name: t.paxstore.us.
‡This is hosted on AWS.
§This is a hosting provider, and IPs are subject to change to allocations within the hosting provider's network.

Internet Domains for UTG Communication

The *.ns.virtualleasedline.net domain is already configured by default during UTG installation. For proper DNS resolution of this domain, all of the Shift4 IP address ranges (listed above) that reference the UTG should be allowed.

Requirement: To ensure that your connection is always routed to the fastest available server, any shortcuts or bookmarks used to access Lighthouse Transaction Manager from a web browser should point directly to www.dollarsonthenet.net, and not to a specific subdomain (such as "server.dollarsonthenet.net").