

IMPORTANT ANNOUNCEMENT FROM SHIFT4

Shift4 data center migration and upgrade COMPLETE!!!

March 10, 2004

Dear Valued Customer,

Last night and into early this morning we completed the scheduled data center migration. No major problems were encountered and other than some minor adjustments, everything went ahead of schedule. We apologize for any inconveniences this migration may have caused and we thank you for your understanding.

While the migration went smoothly on our end, there are two support issues that we are seeing:

- 1) Several of our customers have to manually restart the NetAPI program for it to properly sync up with the new data center. The NetAPI has code to do this task automatically; apparently there are situations that caused this code to fail requiring the manual restart. While this is an easy task, the difficult part is that many of our customers don't know where the NetAPI resides and this makes it difficult to restart the program.
- 2) Several of our customers experienced configuration issues with their firewall / proxy servers. For this reason we have included the firewall / proxy server configuration notes that we included with the prior notifications.

Firewalls & Proxy Servers

\$\$\$ ON THE NET™ and other Shift4 components are 100% reliant on your Internet connection being fully functional. The same holds true for users accessing the \$\$\$ ON THE NET for transaction entry, auditing or reporting via browsers. Firewalls and proxy servers are designed to block your Internet connection in order to minimize the chances that unauthorized personnel will access your computer. They also have the unfortunate side effect of disabling many of the things you might want to do online -- like acquiring online payments - - since these activities depend on your PC making an unimpeded connection to other computers. Therefore, if you are using a firewall or proxy, \$\$\$ ON THE NET may not function properly nor will you be able to access the data for auditing and reporting.

Connecting to different places online requires access through "ports" in your PC's Internet connection, and firewalls and proxies will close certain ports for your

protection. This is not always necessary, but you as the firewall/proxy owner are the only one who can open those ports. We can't do it for you -- but we can give you some tips on how to configure your firewall / proxy so your payment processing will work properly.

What is a firewall or proxy server?

Firewalls and proxies are software programs or pieces of hardware designed to protect your computer and/or network from Internet intruders. Some of these are:

- CheckPoint (hardware/software firewall)
- Cisco Routers (hardware firewall)
- D-Link Routers (hardware firewall)
- Internet Connection Sharing aka ICS - provided by Windows 98SE and higher (proxy)
- Linksys Routers (hardware firewall)
- Norton Internet Security
- Microsoft ISA (proxy)
- Microsoft Proxy Server
- Netscreen (hardware firewall)
- Sygate (proxy)
- Tiny Personal Firewall
- Wingate (proxy)
- ZoneAlarm

Configuring the Firewall / Proxy

If you are behind a firewall/proxy and are able to change its settings, \$\$\$ ON THE NET needs the following TCP ports open in order to function:

- 80 (HTTP port)
- 443 (HTTPS port -- SSL)
- 26880 (NetAPI route port)
- 26881 (NetAPI data port)

In addition, many network administrators lock down firewalls and proxy servers to specific areas of the Internet or specific addresses. Below are a list of all Shift4 and \$\$\$ ON THE NET Internet addresses and ports that your network administrator will need to include in your firewall / proxy exclusion list.

We use the term "exclusion list" with the assumption that your firewall / proxy blocks all URL's, ports and addresses except those in your exclusion list. So by including the previous addresses and ports in your exclusion list, your network administrator is configuring your firewall / proxy to "allow access" to these addresses and ports.

Browser Entry Points

URL	Port	Current IP Address	New Subnet Address	New Subnet Mask
www.shift4.com	80	24.234.30.164 216.250.79.244	(no change)	
www.dollaronthenet.net	80	216.250.79.231 216.250.79.232 209.58.241.41 209.58.241.42	24.120.38.128 67.106.229.32 209.170.218.128	255.255.255.224
info.dollaronthenet.net	443	24.234.71.104 216.250.79.234		
server1.dollaronthenet.net	443	216.250.79.235		
server2.dollaronthenet.net	443	216.250.79.236		
server3.dollaronthenet.net	443	24.234.71.106		
server4.dollaronthenet.net	443	24.234.71.105		
server5.dollaronthenet.net	443	209.58.241.45		
server6.dollaronthenet.net	443	209.58.241.46		
server7.dollaronthenet.net	443			
server8.dollaronthenet.net	443			
server9.dollaronthenet.net	443			
server10.dollaronthenet.net	443			
server11.dollaronthenet.net	443			
server12.dollaronthenet.net	443			

NetAPI Entry Points

URL	Port	Current IP Address	New Subnet Address	New Subnet Mask
ns.virtualleasedline.net	26880	209.58.241.41	24.120.38.128 67.106.229.32 209.170.218.128	255.255.255.224
	26881	209.58.241.42 216.250.79.231 216.250.79.232		
			(same as browser entry points)	

IMPORTANT NOTE #1: If possible, Shift4 highly recommends that port level or domain level (shift4.com, dollaronthenet.net, and virtualleasedline.net) exclusions be used as opposed to IP addresses whenever possible. We realize that not all firewalls / proxy servers allow using domain level exclusions but we urge you to use them if available because of firewall configuration simplicity, load balancing and system fail-over concerns.

IMPORTANT NOTE #2: If you must use IP addresses, the current addresses AND the new addresses will both need to be in your exclusion lists.

Disabling firewalls will not work

Unfortunately, in most cases, firewalls/proxies cannot simply be disabled in order to allow you to use \$\$\$ ON THE NET. Disabling the firewall / proxy will not open the necessary ports. It will simply shut down the firewall/proxy and leave the

ports closed. Also, many factors may conflict with your firewall: Internet Connection Sharing, the use of more than one firewall, or your operating system may all cause conflicts that can impede your use of \$\$\$ ON THE NET and other Shift4 products. To work around these issues, you will need to consult the documentation of your firewall/proxy or contact the manufacturer.

Server to Server API via HTTPS Post Entry Point (SSL)

The server to server entry points will be minimally impacted by this migration BUT may require firewall / proxy server configuration modification to allow access to the new IP address range (see Configuring the Firewall / Proxy and Browser Entry Points above).

Questions and Concerns

If you have any questions or concerns about this scheduled migration and upgrade, please don't hesitate to contact Shift4's 24x7 support department at 702-597-2480 option 2 or e-mail support@shift4.com.