

Implementation Guide for IT

Network Rules

The following is a list of connections that may need to be opened on any firewall systems regulating traffic to/from the bookstore to the outside internet.

Mandatory

1. Outbound UDP traffic to 104.209.214.232 on ports 1171 – 1174. This rule is to allow the cash registers and back office workstations to establish a VPN connection to the point of sale host.
 1. We use OpenVPN for the VPN connections
 2. Client/server communication is encrypted using the AES-256-GCM encryption algorithm
2. The customer is contractually required to provide remote access for the SmartSuite support team when needed.
 1. Zumasys uses the ConnectWise remote support tool to assist customers when they do not have a tool for us to use.
 2. If the firewall rules block the establishment of outbound connections then it will be necessary to allow network traffic for the ConnectWise application.
 - If your firewall appliance supports URL/Alias' then whitelist the following:
 - <https://zumasys.screenconnect.com/>
 - [relay://instance-sisn83-relay.screenconnect.com:443/](https://instance-sisn83-relay.screenconnect.com:443/)
 - Whitelist the following IP addresses if your firewall appliance does not support URL/Alias whitelisting
 - 54.188.209.27 – port 443

- 44.224.173.7 – port 443

3. The customer must provide a reasonable solution for remote support access if the customer is unable, or unwilling, to utilize the ConnectWise application.

3. Vantiv/Worldpay Credit Card Processing

1. This is required to allow on premises cash registers to perform credit card authorization requests via their P2PE devices.
2. If your firewall supports domain based filtering, then you can simply add a rule to allow traffic to <https://transaction.elementexpress.com> on port 443.
3. They round robin through the IP addresses below.
 1. 74.120.156.1 to 74.120.156.254 Port 443
 2. 74.120.157.1 to 74.120.157.254 Port 443
 3. 74.120.158.1 to 74.120.158.254 Port 443
 4. 74.120.159.1 to 74.120.159.254 Port 443

4. Bolt/CardConnect Credit Card Processing

1. This is required to allow on premises cash registers to perform credit card authorization requests via their P2PE devices.
2. Their IP address range is:
 1. 198.62.138.0/24
 2. 206.201.63.0/24
3. An up to date list can be found on their support site:
<https://support.cardconnect.com/bolt/terminal/network-whitelisting>

5. Administrative permissions are necessary to install and configure back office workstations with SmartSuite software.

1. A temporary administrative account can be created for Zumasys use in installing SmartSuite software.
2. A member of the Customer's IT staff can accompany Zumasys staff to each workstation to provide administrative credentials as needed

Optional/Situational

1. Any batch import/export processes will require SFTP access to connect2.total-computing.com (104.209.214.232) on port 4355.
 1. Batch processes include student information, course information, financial aid, etc.
 2. Credentials will be provided during the installation phase.
2. Redshelf ebooks authorizations require access to the following IP addresses on ports 443 and 80.
 1. 34.196.10.62
 2. 34.196.7.198
 3. 34.206.13.124
 4. 5.171.101.186
3. Sender authentication setup for emailed reports, order notification and rental notices originating from the hosting system.
 - These communications are configured with the customer's domain in the "From" address which will trigger spam/junk filters if the steps below are not taken.
 1. Sendgrid Domain Authentication
 - This is completed during the installation and onboarding process and requires the following
 1. Various DNS records to be added to the customer's DNS service
 2. Modification of the customer's SPF, DKIM and DMARC records to include the Sendgrid service as a valid sender
 - If the Sendgrid Domain Authentication is not completed, it may be necessary to whitelist the following domains and IP used by our Sendgrid service. This is not ideal as our customer's end users have an increased chance of not receiving

email communications.

1. 149.72.56.9
2. em94.total-computing.com
3. em1553.total-computing.com

- The system may also be configured to use a customer owned Sendgrid service using their basic SMTP service.

4. Website password reset emails are sent via a second service. This service will ultimately be phased out in favor of the Sendgrid service.

1. 166.70.13.231 – out01.mta.xmission.com
- 166.70.13.232 – out02.mta.xmission.com
- 166.70.13.233 – out03.mta.xmission.com
- 198.60.22.202 – mgr2.xmission.com

Software and Data

Zumasys does not provide any backup services for data stored on hardware at the customer's site. All customer data on the SmartSuite servers is backed up daily for 90 days. Weekly backups are retained for at least 180 days and monthly for one year.

Any removal of data, software or utilities installed during the installation phase will incur a per-hour charge to reinstall and reconfigure. This includes installing any of the above on re-imaged or new/upgraded hardware.

Any in-warranty hardware repairs to hardware provided by Zumasys that removes software or data will not incur the hourly charge to reinstall and configure.

Virus and Malware Protection

Zumasys does not provide or install any Anti-Virus or Anti-Malware software on any customer machines. It is the responsibility of the customer to install, update and run such

products at their own discretion.

Real-time data monitoring programs may need to be configured to exclude certain programs (VPN, Cash Register application) and certain directories if the real time protection features interfere with the day-to-day operations. Zumasys can provide a list of directories, executables and/or services that may need to be added to exclusion lists if real-time monitoring is having an adverse effect on register operations.

Pre-Existing Hardware and Peripherals

Pre-existing hardware is under the customer's responsibility to support. Zumasys staff will do their best to ensure peripherals work within our system, but the ultimate responsibility for unsupported hardware is on the customer. Below is a list of items that fall under the customer's responsibilities to support when they are **not** purchased from Zumasys.

1. Receipt Printers

1. USB and Serial receipt printers are typically compatible as long as they support Epson emulation.

2. Scanners

1. Scanners may need to be programmed to read certain barcode formats.

3. Report Printers

1. The SmartSuite system supports printing to printers that natively support PCL5. Some printers that emulate PCL 5, and some PCL 6 printers, may work. Post Script and other non-PCL based printers are not recommended or supported in any way.

4. Barcode Printers

1. SmartSuite supports printing formats for the following brands. Note that model specific

features or functions may require additional effort to setup and configure.

1. Zebra
2. Datamax
3. Cognitive

5. Inventory scanners

1. Metrologic Scanpal v2 and Tricoder scanners are currently support in SmartSuite.

6. Credit Card Readers

1. Zumasys officially supports credit card readers purchased through Zumasys.

7. Customer displays

8. Programmable Keyboards

9. Cash Drawers

1. Zumasys only supports cash drawers that connect to the receipt printer CD port.