Cashnet Technical Reference Guide

Cashnet provides a comprehensive suite of software as a service (SaaS) products that enable your educational institution to securely process payments over the Internet.

This *Cashnet Technical Reference Guide* contains information about Cashnet's technical infrastructure that is generally of interest to campus system administrators. More detailed information may be obtained upon request.

Contents

Contact & Support

For information and support prior to the implementation process, contact your Cashnet Project Manager.

For post-implementation support, contact Cashnet Support at (800) 231-9182 or Support@Cashnet.com.

Note: For more details about Cashnet Support's services and the process for opening a case, refer to the *Cashnet Support Reference Guide*.

Web Browser Compatibility

To use the Cashnet site, users will require a standard web browser. The following table lists web browser recommendations and requirements depending on Cashnet module and environment.

Table 1: Supported web browsers by module and OS.

CASHNET MODULES	WINDOWS 7	WINDOWS 10	MACINTOSH
Cashnet Administration (Without Peripheral Hardware)	Internet Explorer 11 Firefox 43.0.1 Chrome 46.0 Safari 5.1.7	Internet Explorer 11 Edge	Safari 9
Cashiering with Peripheral Hardware	Internet Explorer 11	Internet Explorer 11	Not supported
***Student Facing Modules (ePayment, eMarket, Checkout)**	Internet Explorer 11 Firefox 42 Chrome 45	Internet Explorer 11 Firefox 42 Chrome 45	Safari 9

** End users can use most browsers with Cashnet; however, only those listed have been fully tested and certified.*

Support for TLS/SSL Protocols

The table below details Cashnet's support the Transport Layer Security (TLS) and Secure Sockets Layer (SSL) protocols for inbound and outbound connections to and from commerce.cashnet.com and train.cashnet.com.

Table 2: Cashnet's support for TLS/SSL protocols.

	SSL 3.0	TLS 1.0	TLS 1.1	TLS 1.2
Outbound	Disabled	Pending disable (date TBD, likely 2018)	Supported starting in CE_2016.3	Supported starting in CE_2016.3
Inbound	Disabled	Disabled in July 2017	Pending disable on March 25, 2018	Supported

Firewall Filtering

In order for your ERP and users to access Cashnet, you must configure your firewall traffic settings and communicate appropriate egress filtering requests to the Cashnet team.

Required Firewall Traffic Settings

Depending on your configurations, please allow the following traffic to pass through your firewall to and from the Cashnet environment.

Table 3: Cashnet firewall traffic settings.

SOURCE	DETAILS	DESTINATION	PORTS
All campus users	Provides browser access to primary and backup Cashnet. Any requests on port 80 are redirected to port 443 before data is entered.	commerce.cashnet.com train.cashnet.com	80 443
All EMV card readers that the campus is using with Cashiering.	Provides access to Monetra UniTerm. Only required if you are using Cashiering stations with EMV-capable card readers.	uniterm.cashnet.com or the following IPs: 34.200.176.140 52.3.139.193 34.192.143.27 34.205.186.34 52.6.56.22 52.71.141.231	8665
34.192.112.253 34.195.213.231	Provides real-time lookup and posting to the ERP system.	Campus ERP system	*As required by your campus ERP system
Any campus systems initiating batch file transfers using SFTP	Only required for batch transfers using SFTP.	34.200.9.186 or eft.cashnet.com	21 or a negotiated high port
Any campus systems initiating batch file transfers using FTP/S	Only required for batch transfers using FTP/S.	34.200.9.186 or eft.cashnet.com	22

* *PeopleSoft using Jolt will always require a range of permitted ports.*

Cashnet Egress Filtering

Cashnet's firewalls are configured to allow outbound traffic to all IP addresses over ports 22 and 443, and high ports. Outbound traffic to any other destination must be explicitly permitted.

Note: All communication through VPN tunnels must be coordinated with the Cashnet Team. This section applies to clients that are not using a VPN.

If you need to have your host added to the allow list, one of your institution's authorized contacts must contact Cashnet Support—via email at Support@Cashnet.com or via phone at (800) 231-9182—and provide your destination hostnames (or IP addresses) and port(s)*. Please note that additions to the allow list can take up to two business days to complete.

Note: IP address ranges, especially in blocks of 16+, will require additional security approval and may take longer than two business days to add.

For users of Amazon Web Services (AWS), we request that you use Elastic Load Balancing.

Because Cashnet egress filtering rules are based on only the underlying IP address and port, note the following:

- If the IP address for a host changes, you will need to ask Cashnet to add the new address to the allow list.
- If the port that Cashnet communicates with changes, you will need to ask Cashnet to add the new address to the allow list, assuming the new port is not always permitted (ports 22, 443, and high ports).
- If Cashnet sends payment notifications to a particular URL and another URL will be added on the same host using the same protocol, you do not need to request an addition to the allow list. For example, the URLs https://erp.myschool.edu/program1.php and https://erp.myschool.edu/program2.pl are the same as far as the Cashnet firewall is concerned.

** Real-time communication with PeopleSoft ERP systems using Jolt will always require a range of ports to be added to the allow list.*

File Transfer Options

Cashnet supports the following transfer protocols (and most transfer clients) for securely transferring batch files between the Cashnet environment and your educational institution. These file transfers include those initiated both by the school and by Cashnet.

- Secure File Transfer Protocol (SFTP)
- File Transfer Protocol over SSL (FTP/S)
- File Transfer Protocol through a Virtual Private Network (VPN)

For detailed information on configuring and automating file transfers to and from Cashnet, refer to our *Secure File Transfers User Manual* in the Support Library.

Domain Name System (DNS)

Cashnet's disaster recovery mechanisms rely on Domain Name System (DNS) to direct web users to a failover site in the event that the primary Cashnet location becomes inoperative. To ensure the least possible disruption in the event of a failover, please follow these practices:

- Do not cache DNS entries longer than the published time-to-live (TTL).
- Always use hostnames, not IP addresses, when accessing Cashnet servers.

Email Notifications & Alerts

Cashnet email services include general notifications as well as alerts on system status.

General Notifications

Depending on the Cashnet modules you purchased and your configuration options, Cashnet will likely send a variety of emails to both your staff and students.

The Cashnet Deployment Team will assist you in configuring the sender address used for these emails. In most cases, these will be addresses from within your own domain. For certain functions, you will also have the option to use a sender address of `notify@cashnet.com`, but replies to this address will not be monitored.

Because Cashnet will send messages to your mail server that claim to be from your own users, your mail server may identify them as spam and try to block them. To ensure that all messages are delivered, you should configure your mail server to accept messages from the following Cashnet mail servers:

- `smtp1.cashnet.com`
- `smtp2.cashnet.com`

If you are required to enter IP addresses for the mail servers, please use the following IPs:

- 34.198.91.107
- 34.198.225.191

To ensure successful delivery to outside mail systems (for example, Gmail or Yahoo), if your institution has a Sender Policy Framework (SPF) record, you should include the Cashnet mail servers in the SPF record. You can do this by adding the following clause:

- `include:cust-spf.cashnet.com`

System Status Alerts

Cashnet uses a mailing list to communicate information about system status and upcoming maintenance to users. We recommend that at least two administrators from each campus join the mailing list.

To join the mailing list, users may send a blank email message to cashnet-alert-subscribe@lists.higherone.com.

To leave the mailing list and no longer receive the Alert Mailing List messages, users can send a blank email message to cashnet-alert-unsubscribe@lists.higherone.com.

VPN Information

Some institutions elect to establish a Virtual Private Network (VPN) between their campus and the Cashnet environment. If your configuration includes a VPN, your project manager will provide you with a questionnaire to gather initial information and then coordinate a phone call with our system administrators to configure the VPN tunnel.

Once the VPN tunnel is established, it generally requires little or no attention. Cashnet will monitor the status of the tunnel and notify your designated VPN contact if it goes down.

If any changes are required to the configuration of the VPN tunnel—such as adding additional servers or changing endpoint equipment—please contact Cashnet Support at least two weeks prior to the change date so that we can make the necessary preparations and coordinate with all relevant parties.

Disaster Recovery & Business Continuity Planning

The Cashnet environment has built-in controls for managing a disaster situation, including a separate disaster recovery location, a failover process, and notifications of a disaster situation.

Capabilities of the Disaster Recovery Site

The disaster recovery site is built to support the same level of activity and same number of users as the primary site. It is designed provide the same response times as the primary site and is able to support the operation of the Cashnet service for as long as necessary.

Data Replication

All transactional data—including payment transactions, MPP, eRefund, and Auto Payment enrollments, setup table updates, and anything else that is viewed through the Cashnet website—is replicated to the disaster recovery site within a few minutes of being updated at the primary location.

Data on the Cashnet secure file transfer servers—such as import files you deliver to Cashnet or NACHA and batch extract files you pick up from Cashnet—is replicated to the disaster recovery site once each day in the early morning hours. If needed, any batch extract or NACHA files can be re-created on demand from the Cashnet End-of-Day screen.

Updates to Cashnet program code are also replicated to the disaster recovery site once each day in the early morning hours.

Failover Process

In the event that the primary site goes down for what appears to be an extended outage, Cashnet will to fail over to the disaster recovery site.

The actual mechanism that directs users to either site is the Internet's Domain Name System, also known as DNS. Normally, when a user asks the DNS servers where to locate Cashnet, the DNS servers respond with the IP addresses of the primary Cashnet site. When Cashnet determines that it is necessary to fail over to the disaster recovery site, Cashnet personnel update the DNS servers to indicate that the Cashnet servers can now be found at a new set of IP addresses, those of the disaster recovery site.

Preparation

Following the instructions below will ensure that your systems are configured properly to make use of the disaster recovery site should it ever become necessary.

- Only connect to Cashnet using the designated hostnames and URLs. Do not connect using an IP address.
- Allow the Cashnet failover site any necessary access through your firewall.
- Do not cache DNS records beyond their stated TTL.

Disaster Recovery Scenario

In the event of a major disruption to the Cashnet primary site, the initial symptoms and what your users will experience will vary depending on the exact nature of the problem.

Cashnet will communicate with users via the Cashnet alert mailing list (p. 5), informing users of the nature of the problem, whether a failover to the disaster recovery site will be initiated, and what the timeframe for recovery is.

If the decision is made to fail over to the disaster recovery site, users attempting to access Cashnet will first see a message that says "Cashnet Disaster Recovery Site," which means failover process is underway and that their web browsers are now connecting to the disaster recovery site. A short time later, users will once again be able to access the site normally as the servers in the disaster recovery site take over processing functions.

The Cashnet alert mailing list will be used to provide updates as appropriate through the disaster recovery process.

Once the issues in primary site been resolved, it will be necessary to "fail back" to the primary location. How long Cashnet will be accessed through the disaster recovery location before returning to the primary location will depend on the nature of the problem in the primary site and could be as little as one day or as long as

several weeks. The switch back to the primary location will occur during Cashnet's normal maintenance window and will be announced in advance via the Cashnet alert mailing list (p. 5).