System Requirements

This section covers system requirements for PearsonAccess[next]. Pearson continually monitors and evaluates the recommended and supported software requirements. As vendors release newer versions of their products, we update the recommended operating systems and browsers accordingly.

> - This document does NOT contain the computer or network requirements for online test delivery using the TestNav test delivery application.
> - TestNav 8 hardware and software requirements are available from TestNav 8 Online Support.
> - For precaching test content browser requirements, see Precache Test Content.

The minimum requirements for all workstations accessing PearsonAccess[next] are listed below.

Browsers	Operating Systems
IE 11	Windows: 7 (with Service Pack 1)
Safari 9	Mac OS X: 10.9, 10.10, 10.11, 10.12
Chrome 49	Windows: 7 Mac OS X: 10.9, 10.10, 10.11, 10.12
Firefox 45	Windows: 7 Mac OS X: 10.9, 10.10, 10.11, 10.12

The current release version for both Firefox and Chrome at the time of our software's release are tested and supported. Newer release versions of Firefox and Chrome should also work, but remember not to make software or technology changes during an online test administration.

Intermediate Network Devices

This section presents guidelines for schools using firewalls and proxy servers when trying to access the PearsonAccess[next] domain only.

Firewall

If there is a firewall between the workstations being used to access PearsonAccess[next] and the Internet, the following destination/protocol/port combinations must be allowed through the firewall:

`*.pearsonaccessnext.com:80`

`*.pearsonaccessnext.com:443`

Proxy Servers/Content Filtering

When accessing PearsonAccess[next], the following URLs must not be blocked on any proxy servers or by any software that is used for Internet content filtering.

`*.pearsonaccessnext.com:80`

`*.pearsonaccessnext.com:443`

Proxy Environments

Many school districts use proxy servers in their network environments. Proxy servers are placed between client nodes and the Internet and are used to forward requests from internal nodes to the Internet. Proxy servers may perform some or all of the following functions:

- Protocol Filtering to control which protocols are forwarded to the Internet
- User Authentication to control who can access the Internet
- Machine Authentication to control which workstations can access the Internet
- Content Filtering to control which Internet content users can access
- Content Caching to speed up access for frequently visited sites

In order for an application to access the Internet in a proxy server environment, the application must know the hostname and port number of the proxy server. Once the application is made aware of the proxy server, it sends all requests for network services to the proxy server for processing. The proxy server receives the incoming requests and must determine what to do with them. If all of the functions listed above have been implemented, the proxy server will:

- Verify that the protocol of the request is serviceable (for example ICMP, UDP, may be blocked by the proxy server).
- Ask user to authenticate that the proxy server does not already recognize the user as being logged in.
- Verify that the source address of the request is on the list of allowed workstations.
- Verify that the requested network object is not blocked by an Internet content filter. (Most Internet content filter vendors provide lists of sites organized by category that administrators can decide to block or allow.)
- Check the proxy server's local disk to see whether the requested object exists in cache. (If the object is in cache, the proxy server will send it directly to the requestor without having to access it from the Internet.)

Assuming that the request passes all of the above steps, the proxy server then stores a record of the request in memory and issues its own request for the same object out to the Internet. When the reply returns to the proxy server, the server matches the reply to the original request stored in memory and forwards the reply to the original requestor.

Email Domain Name

When accessing PearsonAccess[next], school and district email systems must be configured to accept emails from the following address domain: @support.pearson.com