

# TMDS & TSDS Technical Specifications

The following guide provides an overview of minimum and recommended technical specifications for implementing the Texas Math and Science Diagnostic System platform (<http://www.accesstmds.com> and <http://www.accesstsd.com>) in **Low/Standard Security Mode**.

The TMDS & TSDS application has been designed as a 100% web based system in a low security environment. This enables the application to operate in the most minimum of environments. Schools with limited bandwidth and older desktop clients are still able to access and utilize the application.

## Network Specifications

The specifications to the right are indicative of minimum and recommended performance attributes. While we recognize that all facilities will not have immediate access to the recommended network configuration we felt it would be helpful to include this information moving forward.

Network Attribute	Minimum	Recommended
LAN Connectivity	10MB	100MB
Building/Facility Bandwidth	256KB	T-1 Line (1.54MB)
Desktop Bandwidth	56K	128K or better
Routers and Switches	Network Hubs	Cisco 2600 and 2900 Series routers and switches

## Minimum and Recommended Requirements for Testing and Reporting

The following table indicates minimum and recommended technical specifications for desktop PCs and/or laptop computers.

### Testing and Reporting Desktops PC and Macintosh

Hardware	Minimum	Recommended
Desktop PC or Laptop	1 GHz Pentium processor or Apple equivalent	1 GHz Pentium processor or Apple G3 equivalent
Input Devices	Keyboard and mouse	Keyboard and mouse
Memory (RAM)	256 MB	512+ MB or greater
Hard Drive Capacity	No hard drive space is needed	No hard drive space is needed
Web Browser (PC)	Internet Explorer 6.0, Firefox 1.1	Internet Explorer 6.0+, Firefox 1.5+
Web Browser (Mac)	Mozilla Firefox 1.4, Safari 1.3.1	Mozilla Firefox 1.5+, Safari 2.0+
Display	15"+ VGA or better monitor capable of 800x600 resolution or better	17"+SVGA monitor with 1028x768 resolution
Adobe Flash®	7.0. (download free at <a href="http://www.adobe.com/shockwave/download/download.cgi?P1_Prod_Version=ShockwaveFlash&amp;promoid=BIOW">http://www.adobe.com/shockwave/download/download.cgi?P1_Prod_Version=ShockwaveFlash&amp;promoid=BIOW</a> )	9.0 (download free at <a href="http://www.adobe.com/shockwave/download/download.cgi?P1_Prod_Version=ShockwaveFlash&amp;promoid=BIOW">http://www.adobe.com/shockwave/download/download.cgi?P1_Prod_Version=ShockwaveFlash&amp;promoid=BIOW</a> )
Acrobat® Reader	6.0+ (download free at <a href="http://www.adobe.com/products/acrobat/readstep2.html">http://www.adobe.com/products/acrobat/readstep2.html</a> )	7.0+ (download free at <a href="http://www.adobe.com/products/acrobat/readstep2.html">http://www.adobe.com/products/acrobat/readstep2.html</a> )

I have reviewed the table(s) above and our facility meets the minimum technical requirements.

## Desktop Settings

### Computer Protection Software/Firewalls

- Required plug-ins (Adobe Flash™ 7.0+) must be installed prior to activation of computer protection software (MacShield™ or DriveShield™). The system administrator will need to deactivate the Firewall, install the required plug-in (Flash 7.0+) and reactivate the Firewall. (**Note:** DriveShield™ and MacShield™ will automatically restore the computer back to the administrator's pre-defined configuration if plug-ins or downloads are installed following the protection software installation).

**Cookies:** Cookies must be turned **ON**.

Internet Explorer

- Cookies should be set to "accept all cookies". Cache should be set to "1" or the lowest possible setting.
- Check that newest version of stored page is set to "every visit to the page".

Netscape Navigator

- Accept all cookies
- Document in cache is compared to documents on network should be set to "Every Time".
  1. From the Edit Menu, choose Preferences
  2. Click the Advanced category; than click Cache.
  3. Select Once Per Session, Every Time, or Never. "Every Time" assures that the page you see is always the latest.

**Cookies are turned ON.**

### Note on Proxy or Caching Servers

Many customer networks 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 also 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 machines can access the Internet
- Content Filtering* to control which Internet content users can access
- Content Caching* to speed access for frequently visited sites

**A Proxy or Caching server is being used for content filtering.**

**There is a firewall between the workstations and the Internet**

**Content Filtering:** The following URLs must be allowed through any content filters that have been implemented: [www.accesstmds.com](http://www.accesstmds.com).

**Check TCP/http:** Proxy servers and firewalls are configured to allow http on port 80 to the Internet.

**Check User Authentication and Timeout value:** If user authentication is enabled on a proxy server or firewall, the session timeout value should be set to at least be equal to the length of the test (mps at least 60 minutes). This will help prevent users from losing their session with the proxy server or firewall while testing.

**Check Machine Authentication:** if machine authentication is necessary, the proxy server must recognize all machines as valid clients.