## LMASD\_BYOD Wireless Network Connection Help

If you have your own personal device or cell phone and want to connect to a wireless network within a District building, open the wireless network listing on your device and choose **LMASD\_BYOD**. If this wireless network is not listed, select **Add Network**.

While it is not possible to offer a step-by-step guide for all available devices, the information that must be entered to add a network will be much the same as what is included in the Windows 10 connection directions below.

Please note that all devices will ask for a User Name and Password. This is the same User Name and Password that you use to log in to a *school* computer.

## Windows 10

- 1. In Windows, navigate to Control Panel>Network and Internet>Network and Sharing Center.
- 2. Click Set up a new connection or network.
- 3. Highlight Manually connect to a wireless network.
- 4. Click Next.
- 5. Enter the following information on the Manually connect to a wireless network screen:
  - Network name: LMASD\_BYOD (This is case sensitive.)
  - Security type: Choose WPA2-Enterprise

1

- Encryption type: AES
- Check Start this connection automatically
- Check Connect even if the network is not broadcasting
- 6. Click Next.

Enter informatio	n for the wireless network ye	ou want to add
Network name:	LMASD_BYOD	
Security type:	WPA2-Enterprise ~	
Encryption type:	AES ~	
Security Key:		Hide characters
Start this conn	ection automatically	
Connect even i	f the network is not broadcasting	
Warning: If you	a select this option, your computer's p	rivacy might be at risk.

7. Click Change connection settings.

- 8. Click Security tab, then Settings.
- 9. Uncheck Verify the server's identity by validating the certificate.
- 10. Select Secured password (EAP-MSCHAPv2) as the Authentication Method.
- 11. Click Configure.

Protected EAP Properties X
When connecting:
when connecting.
Verify the server's identity by validating the certificate
Connect to these servers (examples:srv1;srv2;.*\.srv3\.com):
Trusted Root Certification Authorities:
AddTrust External CA Root
Baltimore CyberTrust Root
Certum Trusted Network CA
Class 3 Public Primary Certification Authority
COMODO RSA Certification Authority
DigiCert Assured ID Root CA
DigiCert Global Root CA 🗸
< >>
Notifications before connecting:
Tell user if the server's identity can't be verified $$\mathbf{v}$$
Select Authentication Method:
Secured password (EAP-MSCHAP v2)  V Configure
Enable Fast Reconnect     Disconnect if server does not present cryptobinding TLV     Enable Identity Privacy

- 12. Uncheck Automatically use my Windows logon name and password (and domain if any).
- 13. Click **OK.**

EAP MSCHAPv2 Properties	l	×
When connecting:		
Automatically use my W password (and domain	<i>l</i> indows logon name if any).	e and
ок	Cancel	

- 14. Click **OK**.
- 15. From the **Security** tab, click **Advanced Settings**.

ecurity type:	WPA2-Enterprise	~
ncryption type:	AES	~
licrosoft: Protected I	EAP (PEAP) v	Settings
Microsoft: Protected I → Remember my cre	EAP (PEAP) ~	Settings ion each

- 16. Select the **802.1X settings** tab.
- 17. Check Specify authentication mode:
- 18. Choose User authentication.
- 19. Click Save credentials.

Enable single sign on for this network   Perform immediately before user logon  Perform immediately after user logon  Maximum delay (seconds):  Allow additional dialogs to be displayed during sing sign on  This network uses separate virtual LANs for machin and user authentication
Perform immediately before user logon     Perform immediately after user logon     Maximum delay (seconds):     10     Allow additional dialogs to be displayed during sing     sign on     This network uses separate virtual LANs for machin     and user authentication
Perform immediately after user logon Maximum delay (seconds):     10     In     Allow additional dialogs to be displayed during sing     sign on     This network uses separate virtual LANs for machin     and user authentication
Maximum delay (seconds): 10 Allow additional dialogs to be displayed during sing sign on This network uses separate virtual LANs for machin and user authentication
<ul> <li>Allow additional dialogs to be displayed during sing sign on</li> <li>This network uses separate virtual LANs for machin and user authentication</li> </ul>
This network uses separate virtual LANs for machin and user authentication

20. Add your User Name and Password (the same User Name and Password you use to log into a *school* computer).

١	Windows Security	×
2	Save credentials	
	Saving your credentials allows y the network when you're no download updates).	your computer to connect to ot logged on (for example, to
	User name Password	

21. Click **OK** three times and then **Close**.

## Apple I-phone

- 1. Go to Settings Wifi
- 2. Select LMASD\_BYOD
- Your username and password are the ones you use to log into the school machines with (Students Username = First five of last name and first three of first) (Teachers Username = First initial of first and up to seven of last)

Ill Extended 1x	12:20 PM	୶ ∦ 68% ■.
Enter	the password for "LMASD	_BYOD"
Cancel	Enter Password	Join
Username		
Password		

4. When it asks about the certificate touch "Trust" in the upper right portion of the screen

No Service	12:21 PM	1 🕴 67% 🔳 י
Cancel	Certificate	Trust
	Example Server Certin Issued by Example Certif	<b>ficate</b> icate Authority
	Not Trusted	
Expired	12/20/17, 9:24:15 AM	
More Det	ails	>

5. This will get you connected. If it does not work the first time, try one more time before entering in a helpdesk ticket.

## Android

1. Go to and select LMASD\_BYOD



DETAILS DONE

2. Tap on Select Certificate and choose "Don't Validate"

<b>F</b> (		\$ €	84% 🗎 12:28	PM
	LMASD_BYOD			
	EAP method			/
	PEAP 🔻			ım
	Phase 2 authentication			
	None 🔻			
0 1	CA certificate			
Т	Select certificate			53
-	Don't validate	۰d.		
	CA	NCEL	CONNECT	

3. Scroll down to enter your Identity (username) and password.

LMASI	D_BYOD	
Anonym	ous identity	
Passwo Enter p	<b>rd</b> bassword	
$\bigcirc$	Show password	
	Auto reconnect	
$\bigcirc$	Show advanced options	

4. Tap Connect

Please use these directions as a guide and, if further assistance is needed, please contact a Building Technology Coordinator.