User cannot connect to Member WiFi

09/29/2020 02:55:00

FAQ Article Print

Category:	Customer	**Votes:**	0
State:	public (all)	**Result:**	0.00 %
Language:	en	**Last update:**	17:57:18 - 11/01/2018

Keywords

wifi meraki tgr

Symptom (public)

User cannot connect to network services via Wi-Fi (Internet, email, printing etc)

Problem (public)

User device has not been configured for access to Member Wi-Fi

Solution (public)

Windows 10

The following steps will configure a Windows 10 client to use 802.1X with Meraki-hosted RADIUS (NOTE: these are instructions for the 802.1X with Meraki-hosted RADIUS only. Customer-based RADIUS server configuration requirements are specific to the customer's own RADIUS server and can vary widely):

- Click the "Start" menu
- Navigate to Settings (Gear Icon) > Network & Internet > Wi-Fi > Manage Known Networks
- Click 'Network and Sharing Center'
- Select 'Set up a new connection or network'
- Select 'Manually connect to a wireless network'
- Enter the SSID name in the 'Network name:' field
- Select 'WPA2-Enterprise' in the 'Security type:' drop down
- Select your encryption type from the 'Encryption type' drop down
- Click 'Next'
- When 'Successfully added' appears click 'Change connection settings'
- Select the 'Security' tab
- Click the 'Advanced settings' button
- On the '802.1x settings' tab, check the box 'Specify authentication mode' and choose 'User Authentication' from the drop down
- Click 'OK'
- Back on the 'Security' tab, make sure 'Choose a network authentication method' is set to 'EAP (PEAP)' and then click the 'Settings' button
- Click 'OK'
- For 'Protected EAP Properties' uncheck 'Validate server certificate' or if you choose to validate server certificate make sure 'Go Daddy Class 2 Certification Authority' and/or '[1]http://valicert.com' is checked in the 'Trusted Root Certification Authorities' list.
- Click the 'Configure' button
- Uncheck 'Automatically use my Windows logon name'
- Click 'OK' to close all the open dialog boxes

Apple macOS

The following steps will configure a macOS client to use 802.1X with Meraki-hosted RADIUS (NOTE: these are instructions for the 802.1X with Meraki-hosted RADIUS only. Customer-based RADIUS server configuration requirements are specific to the customer's own RADIUS server and can vary widely):

- Go to System Preferences => Network => AirPort => Advanced => 802.1X
- Click the "+" button in the lower left corner of the screen to add a new user profile
- Enter your user name and password given to you by your network administrator into the fields to the right.
- Select your network from the drop down list of menus
- Make sure TTLS and PEAP checkboxes are selected
- Click "OK"
- You should now be able to connect to the network.

Android

The following steps will configure an Android client to use 802.1X with Meraki-hosted RADIUS (NOTE: these are instructions for the 802.1X with Meraki-hosted RADIUS only. Customer-based RADIUS server configuration requirements are specific to the customer's own RADIUS server and can vary widely):

- Go to Settings > Wi-Fi
- Open the options menu by clicking the context menu button:

Note: This step may vary by device, or on tablets. The Add Wi-Fi option may not be hidden behind a context menu.

- Select Add Wi-Fi
- Enter the Network SSID name and choose 802.1x EAP from the Security drop-down menu
- Choose PEAP from the EAP method drop-down menu
- Choose MSCHAPV2 from the Phase 2 authentication drop-down menu
- Enter the domain and username in the Identity field. Use the domain/username format
- Enter the password for the corresponding username in the password field
- Optionally, check the Show Password check-box to verify that the password was entered correctly
- Press Save in order to save the changes

Windows 8

Unlike previous versions of the OS, Windows 8 will not attempt to automatically use local credentials for wireless connections. As such, associating with an 802.1x-protected SSID consists of simply connecting to the network, as outlined below:

- Navigate to the Desktop.
- Select the wireless network icon on the lower-right hand of the screen.
- Select the intended SSID on the right.
- Check/uncheck the Connect automatically option as intended, and press Connect.
- Enter the email address and password of the Meraki RADIUS user, in the User name and Password fields respectively.
- Select Connect.
- If prompted about a certificate warning, select Connect again.

Windows Vista

The following steps will configure a Windows Vista client to use 802.1X with Meraki-hosted RADIUS (NOTE: these are instructions for the 802.1X with Meraki-hosted RADIUS only. Customer-based RADIUS server configuration requirements are specific to the customer's own RADIUS server and can vary widely):

- Go to Start and enter "Network and Sharing Center".
- Click "Set up a connection or network".
- Click "Manually connect to a wireless network".
- Enter the SSID (case sensitive).
- Choose WPA2-Enterprise and AES.
- Check "Start this connection automatically" and "Connect even if the network is not broadcasting" (for hidden SSIDs).
- On the next screen, choose "Change connection settings".
- On the Connection tab, check only the boxes "Connect automatically when this network is in range" and "Connect even if the network is not broadcasting" (for hidden SSIDs).
- On the Security tab, make sure "WPA2-Enterprise" and "AES" are selected as well as "Microsoft: Protected EAP (PEAP)". Click Settings.
- Uncheck "Validate server certificate".
- Click "Configure" and uncheck "Automatically use my Windows logon name and password (and domain if any)". Click OK three times.
- Now click "Connect to network", select your SSID from the list, and "Enter/select additional log on information".
- Here you enter the username and password which are configured on the Configure->Users page on the dashboard. Click OK.
- You should now be successfully connected.

Windows 7

The following steps will configure a Windows 7 client to use 802.1X with Meraki-hosted RADIUS (NOTE: these are instructions for the 802.1X with Meraki-hosted RADIUS only. Customer-based RADIUS server configuration requirements are specific to the customer's own RADIUS server and can vary widely):

- Click the "Start" menu.
- Navigate to Control Panel>Network and Internet>Network and Sharing Center>Manage Wireless Networks.
- Click "Add".
- Select "Manually create a network profile".
- Enter the SSID name in the "Network name:" field.
- Select "WPA2-Enterprise" in the "Security type:" drop down.
- Select your encryption type from the "Encryption type" drop down.
- Click "Next".
- When "Successfully added" appears "Click Change connection settings".
- Select the "Security" tab.
- Click the "Advanced settings" button.
- On the "802.1x settings" tab, check the box "Specify authentication mode" and choose "User Authentication" from the drop down.
- Click "OK".
- Back on the "Security" tab, make sure "Choose a network authentication method" is set to "EAP (PEAP)" and then click the "Settings" button.
- For "Protected EAP Properties" uncheck "Validate server certificate" or if you choose to validate server certificate make sure "Go Daddy Class 2 Certification Authority" and/or "[2]http://valicert.com" is checked in the "Trusted Root Certification Authorities" list.
- Click the "Configure" button.
- Uncheck "Automatically use my Windows logon name".
- Click "OK" to close all the open dialog boxes.

Windows XP

The following steps will configure a Windows XP client to use 802.1X with Meraki-hosted RADIUS (NOTE: these are instructions for the 802.1X with Meraki-hosted RADIUS only. Customer-based RADIUS server configuration requirements are specific to the customer's own RADIUS server and can vary widely):

- Switch to a network other than the one you want to configure (otherwise

Windows will not retain your changes).
- Go to Control Panel -> Network Connections -> Wireless Network Connection
- Click on Properties, go to "Wireless Networks" tab
- Find the network name under the "Preferred Networks" list, click Properties, click Authentication tab.
- For "EAP type", choose PEAP. (The default is "smart card or other certificate" which will not work).
- Still on the Authentication tab, uncheck the "Authenticate as computer when computer information is available" box.
- Click Properties under PEAP.
- Under 'Trusted Root Certification Authorities', scroll down to "UTN-USERFirst-Hardware" and check that box.
- Still under 'Trusted Root Certification Authorities', scroll down to "Go Daddy Class 2 Certification Authority" and/or "[3]http://www.valicert.com" and check those boxes.
- Make sure the "do not prompt user to authorize new servers...." box is unchecked.
- Under "select authentication method", make sure that "EAP-MSCHAPv2" is selected. Click the "configure" button next to it, and uncheck the "Automatically use my Windows logon name..." box.
- Click OK to close all the open dialog boxes.

[1] http://valicert.com/
[2] http://valicert.com/
[3] http://www.valicert.com/