Repairing UCONN-SECURE Wireless on Windows

This article is for when you've used the set-up or fix articles to set-up or fix UCONN-SECURE, and they did not resolve the issue. It addresses multiple problem areas in order of wall to computer, and includes commonly used tricks that have worked in the past.

We assume:

- You either have a 169 IP or a Media State Disconnect.
- You do not have a Static IP.
- You've reached this point through the Windows UCONN-SECURE Fix checklist.
- You've tried deleting and reconfiguring UCONN-SECURE.
- You've checked Windows Firewall (Try turning the firewall off. Does wireless work?).
- You've already reset the NetID.
- You don't believe it could be malware.

It might be malware if:

- Firewall cannot be enabled.
- You find suspicious programs in appwiz.cpl, msconfig, System Files, or Task Manager.
- Have a shop lead do a quick check if you're unsure.

NetID Account Troubleshooting

Reset NetID password

- Despite client's knowing their NetID, changing their password can solve the issue.
- Having the client change their password should be the first step.

Failing NetID

- Remove the client profile by going to Command Prompt and typing "netsh WLAN delete profile name= UCONN-SECURE".
- Use your own NetID to configure UCONN-SECURE. If this works, you know there is an issue with the client's NetID.
- To remove your NetID after trying it, go to Command Prompt and type "netsh WLAN delete profile name= UCONN-SECURE".

LDAP Status

Check that the client has a true LDAP status.

- Have the client go to NetID webpage.
- Have the client select Password Test from NetID Tools.
- If the client is not logged in, they will be brought to the NetID Single Sign-On Page. Have the client sign in.
- Client will now be brought to the password test webpage. Have the client enter their password.
- You can check the status of UCONN-SECURE. Active Directory and OpenLDAP & Kerberos.
- If any of these categories are not listed as synchronized, a password reset should synchronize all the categories.

Password Wait Time

In theory sometimes NetID passwords take 24 hours to reset. Though we have never seen this in practice.

Device Manager

This step is unnecessary if you can connect to another network.

- In Device Manager, double-click Network Adapters.
- Then double-click the wireless network adapter.
- In the General tab it will tell you if the device is working properly.
- If the adapter is not working properly, click on the Driver tab, and there you can update the driver, disable, or uninstall it.

Third-Party Wireless Programs

- For Windows 7, 8, and 10, most machines do not come installed with a third party wireless assistant, therefore you should not have any issues. However the exception may be some older Lenovo machines.
- If a third party wireless assistant is present, the wireless networks tab will not be present in the Wireless Network connection properties window.
- When you have located the third party wireless assistant, make sure you have unchecked Let this tool manage your wireless networks. Different managers will phrase this differently. Then restart the machine, the wireless networks tab should be visible. Proceed with setting up UCONN-SECURE as usual.
Anti-Virus and Firewall Programs

- In appwiz.cpl search for anti-virus programs such as McAfee, Norton, Kaspersky, AVG, PC Tools, SpywareDoctor, ClamWin, or Avast.
- The reason why UCONN-SECURE may not connect is because there is an authentication issue caused by Symantec.
- If any of the previously listed programs are installed on a Windows machine, please remove them and enable Windows Defender.

Trusted Root Certificates

Checking Trust

- Type “certmgr.msc” into the Start Menu.
- In the left side menu, click Trusted Root Certification Authorities Certificates.
- Double-click AddTrust External CA Root.
- Under the Details tab, click Edit Properties.
- In the General tab, make sure Server Authentication is checked.
- Click OK twice.
- Repeat this for UTN-UserFirst-Hardware.

Installing Certificates

- Use a shop USB, which should have the certificates on it.
- In Certificate Manager, click on Trusted Root Certification Authorities. Make sure this is highlighted.
- Click Action All Tasks Import.
- A Wizard window should come up with instructions for importing certificates.
- Once certificate(s) is/are installed, make sure to go back and check their trust.

Accessing files through peer-to-peer services

If a class requires you to obtain files through a torrent or other types of peer-to-peer communication, you must use a wired connection.

Related Articles

- Mapping the Q: Drive on Windows
- Using SafeAssign in HuskyCT
- Accessing the UConn Network Through a VPN Client
- Accessing the UConn Network Through a Web Browser
- Using Calendar in Outlook for Windows