# IT 202 Project Two Knowledge Base Document Template

Complete this template by replacing the bracketed text with the relevant information. Repeat these steps for each user problem that you want to create a knowledge base document for.

## Gather Information

Users cant access SharePoint website.

## Identify What Has Changed

Nothing has changed in the system to the users knowledge.

## Create a Hypothesis

We need to verify the network adapter, as it might not be connected to the user's computer?

Does the computer have physical connectivity?

If network has physical connection, does it have IP configuration?

Does the device have a ping to show connectivity is working?

## Determine the Appropriate Fix

Verify network adapter by checking icon for wi-fi and make sure it is enabled. If there is no icon than we need to check the device manager and see if it is detected. Then make sure it has the appropriate drivers and is enabled (TestOut LabSim, n.d.).

To check to see if wireless network has connection we look at the icon to see if it has an X on it indicating it is not connected. We need to make sure the network interface card is installed properly and has necessary antennae installed. Also, verify the SSID is settings are correct and if MAC address filtering is being used that the device is configured onto the access point. Another step to be taken is to see if connection is poor by using a wireless analyzer to locate wireless networks, spot crowded channels or sources of interference, and locate areas with bad wireless coverage (TestOut LabSim, n.d.).

To verify the IP is configured go to command prompt and type in ipconfig to view the IP address, subnet mask, and default gateway for the system. Next, verify if the computer is configured to the DHCP server for automatically assigning IP addresses. If the IP address on the machine is assigned 169.254 and subnet mask was assigned 255.255.0.0 then the operating system is not connected to the DHCP server and is instead using APIPA. We would contact our network administrator who is responsible for the DHCP server to know if the server is down or unreachable. We do an ipconfig/release command to get rid of all statically assigned addresses. Then we type ipconfig/renew for DHCP discovery packets (TestOut LabSim, n.d.).

Use ping to test the connectivity in the network with other network hosts. If the destination device sends back an answer from the request you know that it is configured correctly (TestOut LabSim, n.d.).

## Implement the Fix

The network adapter is working as the icon is showing Wi-Fi connection. Also, the Wi-Fi was already enabled.

The NIC is installed properly and the SSID settings are correct. The device has been configured correctly on the access point, as MAC filtering was being used but is not issue as it connects to the access point. We also used the wireless analyzer to check for locating wireless networks, identifying crowded channels, finding locations with poor wireless coverage, detecting rogue access points, and sources of interference.

We checked the network for ipconfig under the command prompt and found the IP address was 169.254.1.0 and the subnet mask was 255.255.0.0 indicating this was not connecting to the DHCP server. We contact out network administrator to see if the DHCP server was down or unreachable. The DHCP server was only down so now we type ipconfig/release to get rid of statically assigned addresses. Then we type ipconfig/renew for DHCP discovery packets. We now have DNS server configured as well with the correct IP address, subnet mask, and default gateway for this network segment.

Next we ping 10.10.10.1 to request a ICMP echo request and receives a ICMP echo response packet that verifies we have connectivity between the two hosts.

## Gather Information

Users gets blue screen when loading the system.

## Identify What Has Changed

The recently upgraded their system to windows 10.

## Create a Hypothesis

The system may have incompatible hardware installed on the system?

The hardware of the driver could be out of date?

The BIOS could be out of date?

Maybe certain hardware components are not fully intact and pushed in all the way into their slots?

## Determine the Appropriate Fix

We check the manufacturers website to make sure all hardware is compatible with the operating system (TestOut LabSim, n.d.).

We check the hardware driver to see if it needs to be updates in the device manager settings.

We check the BIOS setting to see if the BIOS is out of date.

Check to see if the hardware components are fully installed and pushed into their designated slots, if they aren't then the BSOD is likely to occur (TestOut LabSim, n.d.). We need to check for loose hardware/cables, unseated hard drives, and RAM chips.

## Implement the Fix

All hardware is compatible on the manufacturers website with are current hardware.

The hardware driver is up to date under the safe mode settings of the current system.

The BIOS settings is up to date under the safe mode settings.

The hardware components are not all intact as the RAM chips were not pushed all the way in. This is likely to be causing the BSOD. The user tests the operating system to see if it works effectively as there is no more BSOD.

## Gather Information

HOU security console is not allowing login.

## Identify What Has Changed

Nothing has changed that the user knows.

## Create a Hypothesis

Is the user in range of the access point?

Is the configuration for the SSID and WEP/WPA keys correct?

There is a thin configuration so we need to make sure that the AP can communicate with the wireless controller?

Does the wireless network have a compatible wireless card that uses the same standard?

Is there channel interference?

## Determine the Appropriate Fix

To see if user is in range check how far the device is from the AP and look at the manufacturers website to see how far it can support.

The configuration of the SSID is correct because we can see the network we want to connect to. and WEP/WPA keys are correct by checking WI-FI protocol and seeing that you need a passphrase to access the network.

To check if configuration of the AP can communicate with the wireless controller we go to the website of the WLC through HTTP and login (Mills, 2022). Click wireless and known rogue APs. Next, look at status and make sure it says known (“Trusted AP Policies on a Wireless LAN Controller”, n.d.). This confirms the AP is communicating with the wireless controller.

To see if the wireless network is using the same standard as the wireless card you can check the manufacturers website of both wireless network and wireless card. Also, you can go to WI-FI status and click information to see the standard (Mills, 2022). On the wireless card you can look for the description which will tell you.

Channel interference can be solved by changing the channel used on the access point (TestOut LabSim, n.d.). If the area has different wireless networks, we can configure each with a different channel, with at least two channels separating the channels in use (TestOut LabSim, n.d.).

## Implement the Fix

The user is within 100 feet of the AP. The manufacturers website says it can support 200 feet.

The SSID is visible and can connect to with no problem. We are correctly entering in the passphrase for the WEP/WPA.

We looked at the manufacturers website of the Wireless LAN Controller. We went under the known rogue APs and see our AP.

We went to WI-FI status information to see what standard it was using it was 802.11g and the wireless card is using 802.11g.

There was additional interference as our STN ratio was low making it acceptable to interference. We changed the AP channels to 1. The secuirty console will now allow the user to login. The interference could have been caused by a microwave, game controller, or Bluetooth devices.

## Gather Information

User wants to add capabilities to the DocuSign to be able to send documents for signatures.

## Identify What Has Changed

Nothing has changed to the operating system that user knows.

## Create a Hypothesis

DocuSign is not allowed for signatures because it can alter documents and signatures.

DocuSign is not allowed signatures because it generates a fake handwritten image that seems untrustworthy.

Does the company trust the software of DocuSign to get peoples signatures?

## Determine the Appropriate Fix

The signing of a signature is linked to an email address and IP address for validation of the signature (“An Introduction to DocuSign Legality and Security”, n.d.).

The contents of the document cannot be changed after it has been signed by the authenticated party (“An Introduction to DocuSign Legality and Security”, n.d.).

DocuSign gives users an audit trail to track everything such as where it was viewed, timestamps, email addresses, and IP addresses (“An Introduction to DocuSign Legality and Security”, n.d.).

## Implement the Fix

When sending a document we were able to link it to an employee’s email address and IP address for validation for the signature.

After signed from the employee we forwarded the document to we see no changes have been made to the document.

We tracked users audit track for further validation and were able to find when they viewed the document, timestamps, IP addresses, and email addresses. We were able to validate everyone from inside the company by email address and IP addresses verifying their signatures.

## Gather Information

Error loading operating system.

## Identify What Has Changed

The user is not aware of anything different that could have affected the operating system.

## Create a Hypothesis

the computer SATA drive could be a higher number than the computer normally starts at like SATA 0?

the computer booting from a removable drive first, if that USB drive does not have anything downloaded for the operating system upon boot?

the boot drive is unplugged causing it to not be recognized by the BIOS or UEFI which can cause the same error?

The system could have memory issues by mixing old and new memory modules? The system could tell us what is happening by looking at the error message by using the manufacturers documentation?

Our master boot record could be corrupt or overwritten?

## Determine the Appropriate Fix

If the system is booting from the wrong SATA drive you can go into the BIOS and change it to SATA 0 (TestOut LabSim, n.d.).

If it is booting from the USB drive you can again go into the BIOS and change which drive you want the operating system to load first.

If the boot drive is unplugged we can plug it in and see if the BIOS or UEFI recognize the boot drive and see if the error goes away (TestOut LabSim, n.d.).

If the memory modules are causing the problem then we need to replace all old memory modules with new ones. If there is a memory problem the system would tell us it is a 201 error (TestOut LabSim, n.d.).

The master boot record can be fixed by writing commands in the command prompt in this order:

Bootrec / fixmbr: Repairs the master boot record.

Bootrec / fixboot: Repairs the boot sector.

Bootrec / rebuildbcd: Rebuilds the boot configuration data (TestOut LabSim, n.d.).

## Implement the Fix

We went into the BIOS settings to change the SATA drive to the appropriate SATA 0 so it would load, but it was already loading from SATA 0 with the appropriate drive.

We looked to see if the computer was first booting from a USB drive, this was not the case as it had the appropriate drive.

We checked to make sure the boot drive was plugged in and see if the BIOS or UEFI recognize the boot drive, but the error still remained and the boot drive was plugged in.

The system displays a 201 error code which indicates a memory problem on the system. We replaced all old memory modules with new ones, as the old memory modules were not compatible with the system, the user must have had a memory upgrade but did not check to make sure it was compatible with the system.

We checked the master boot records and entered the commands but the system does not load. The master boot records are not corrupted or overwritten as these commands would have solved that problem.

**References**

*An Introduction to DocuSign Legality and Security*. (n.d.). @PDFelement. Retrieved September 27, 2022, from <https://signx.wondershare.com/comparison/docusign-legality-security.html#:~:text=In%20a%20way%2C%20DocuSign%20is%20the%20single%20legal>

Mills, M. (2022, August 29). *Check which Wi-Fi version your wireless network card supports | ITIGIC*. Itigic.com. <https://itigic.com/check-which-wifi-version-your-wireless-network-card-supports/#:~:text=In%20the%20description%20of%20the%20network%20card%2C%20we>

*Trusted AP Policies on a Wireless LAN Controller*. (n.d.). Cisco. Retrieved September 27, 2022, from <https://www.cisco.com/c/en/us/support/docs/wireless-mobility/wlan-security/100368-trustedAP.html#:~:text=Complete%20these%20steps%20in%20order%20to%20verify%20that>

*TestOut LabSim*. (n.d.). Labsimapp.testout.com. Retrieved September 27, 2022, from <https://labsimapp.testout.com/v6_0_514/index.html/productviewer/242/3.4.2/26bac963-80a8-4aa4-a744-b41803c97939>