

SILICONCHIP TECHNOLOGIES

USER GUIDE

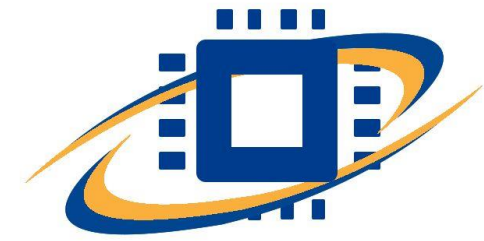
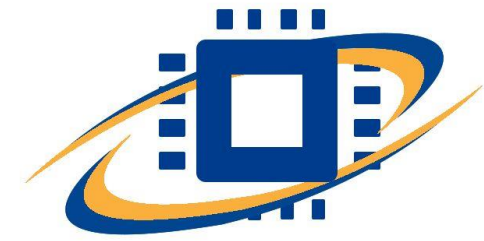


TABLE OF CONTENTS

- Introduction
- Connecting to the Chipedge Labs
- Installing & Configuring VPN
- Connecting to VPN
- Usage Limits & Other Details.
- Do's & Don't
- Common errors and how to fix
- IT Helpdesk & Escalation system

INTRODUCTION TO SILICONCHIP TECHNOLOGIES

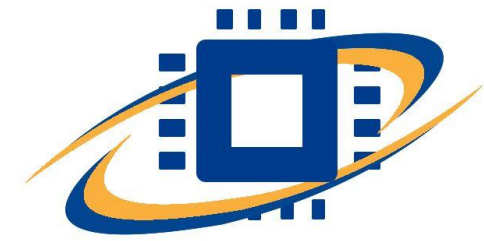


Welcome to SiliconChip Technologies

With a goal to provide best Learning Experience to our Students & learners, we have designed our lab infrastructure with best possible servers, high end data center, high quality internet leased lines, Synopsys EDA Tools & different applications.

And particularly best in class ticket-based IT Helpdesk, to provide high quality IT Support.

We at ChipEdge will continue to strive to improve the learning experience, by continuously improving our infrastructure & support system. We request your help, to provide sincere feedback on how we can improve further.

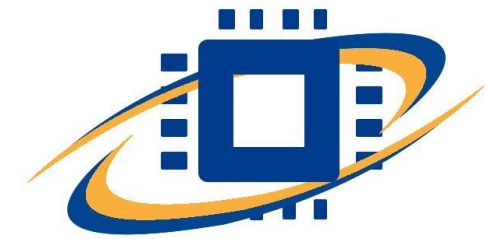


CONNECTING TO SILICONCHIP TECHNOLOGIES

Accessing SiliconChip Technologies is a two-step process

Step1: Connecting to Forticlient VPN

Step2: Login to server with Remote desktop connections (Windows feature) / Remmina (Ubuntu feature)



VPN INSTALLATION







- Download VPN client from <https://www.fortinet.com/support/product-downloads#vpn>
- Under Forticlient VPN, choose your OS version to download the software
- Open/run the saved file **“FortiClientVPNOnlineInstaller”**

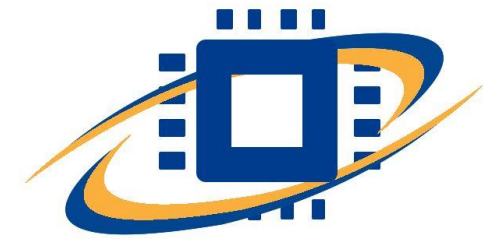
FortiClient VPN

The VPN-only version of FortiClient offers SSL VPN and IPsecVPN, but does not include any support. Download the best VPN software for multiple devices.

Remote Access

- ✓ SSL VPN with MFA
- ✓ IPSEC VPN with MFA

 Download VPN for Windows DOWNLOAD	 Download VPN for MacOS DOWNLOAD	 Download VPN for Linux DOWNLOAD .rpm
 Download VPN for iOS DOWNLOAD	 Download VPN for Android DOWNLOAD	 Download VPN for Linux DOWNLOAD .deb



CONFIGURING THE VPN

- After opening the application click on **"Configure VPN"**
- connection name: any name like **"chipedge-VPN"**
- description: any name like **"chipedge-VPN"**
- Give the remote gateway as **180.179.249.110**
- Select **"customize port"** option
- Update the port number with **10443**
- Select **"Prompt Login"** under Authentication
- Click on Save

New VPN Connection

VPN: **SSL-VPN** | IPsec VPN | XML

Connection Name: chipedge-VPN

Description: chipedge-VPN

Remote Gateway: 180.179.249.110

+Add Remote Gateway

☒ Customize port 10443

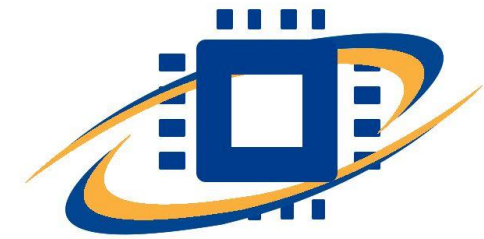
☐ Enable Single Sign On (SSO) for VPN Tunnel

Client Certificate: None

Authentication: ☒ Prompt on login ☐ Save login


☐ Enable Dual-stack IPv4/IPv6 address

Cancel Save



CONNECTING TO THE VPN

- Enter the VPN username and password as provided to you.
- Click on **Connect**
- At 40% you will receive a security alert, click on **Yes** and continue



Status: 40%

VPN Name chipedge-VPN

Username test1

Password

Disconnect



VPN Name chipedge-VPN

IP Address 10.212.123.28

Username test1

Duration 00:01:16

Bytes Received 0 KB

Bytes Sent 40.51 KB

Disconnect

Security Alert

A secure connection with this site cannot be verified. Would you still like to proceed?

The certificate you are viewing does not match the name of the site you are trying to view.

Yes No View Certificate More Info

Status: 40%

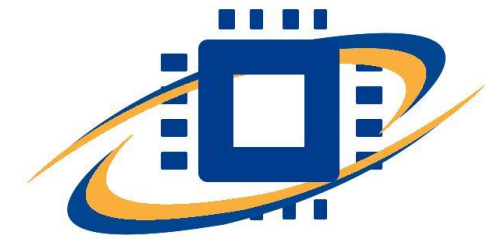
VPN Name chipedge

Username test1

Password

☐ Auto Connect ☐ Always Up

Disconnect



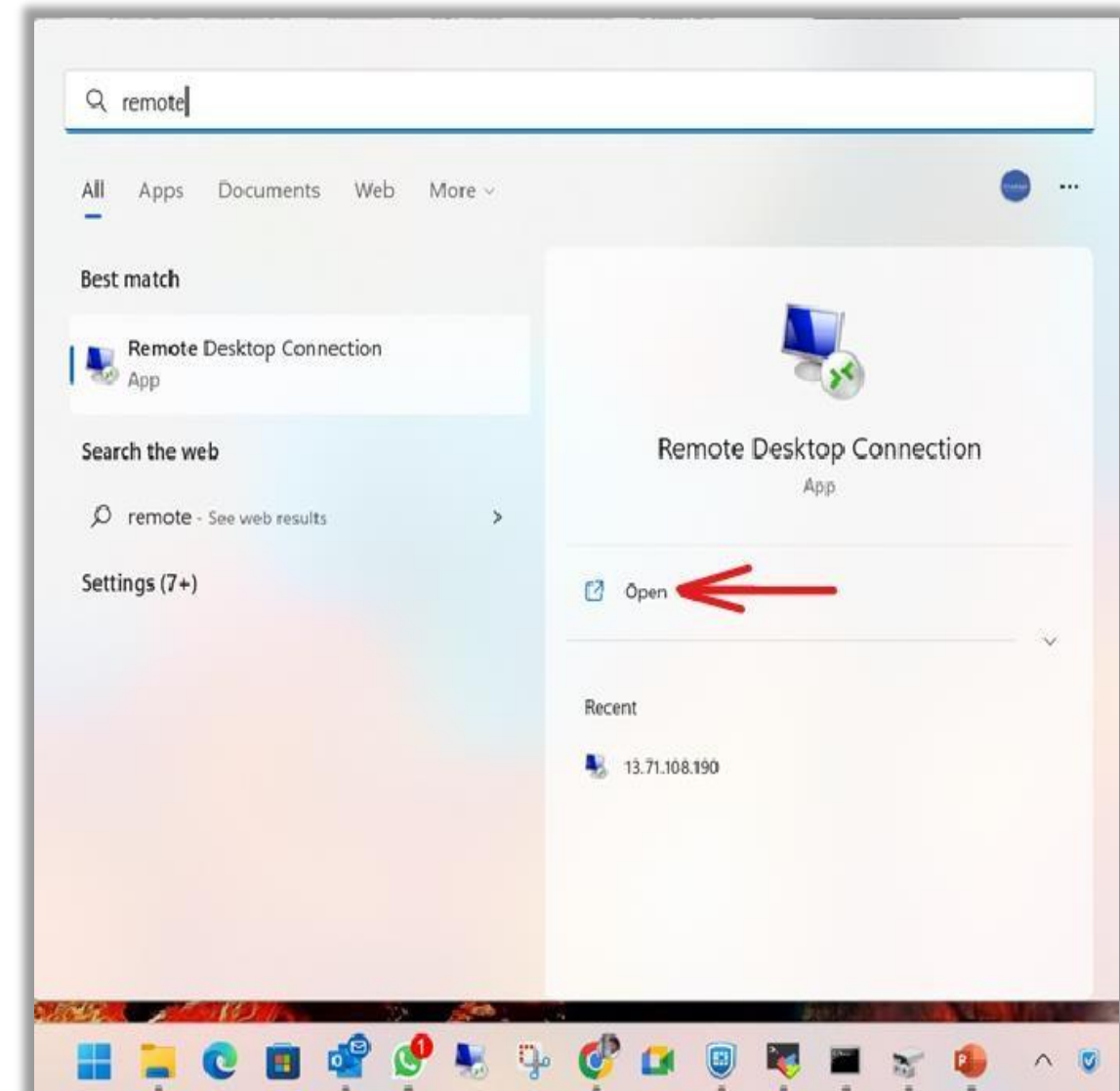
CONNECTING TO THE SERVER

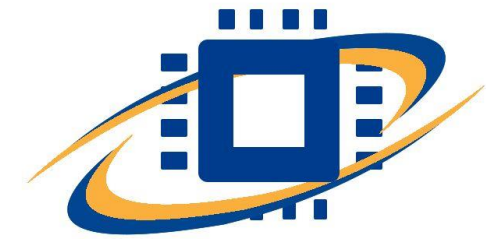
After you are connected to the VPN, open the Remote Desktop Client

Windows machine: Open **Remote desktop Connection** application which is available in all Windows 7/10/11 OS.

Click on Windows **START** button >> search for **Remote Desktop Connection**

Linux machine: click the Main Menu button in the GNOME interface of Ubuntu, find the Remmina icon in the menu or type **Remmina** to locate the application. You can also open the console (terminal) and enter **remmina** to execute the application.



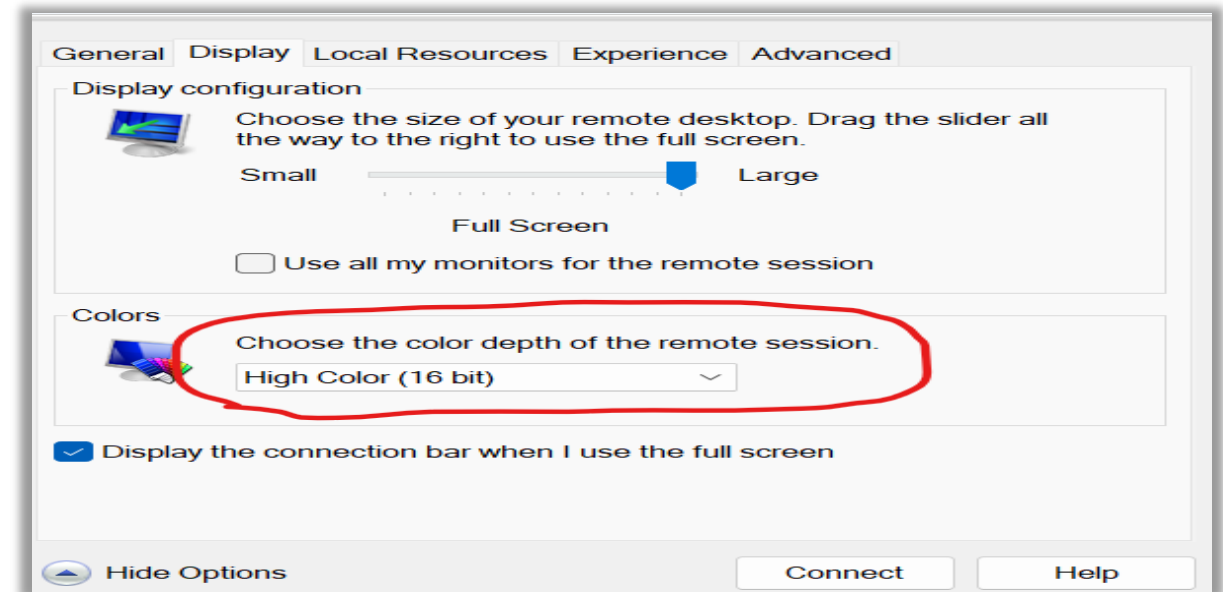
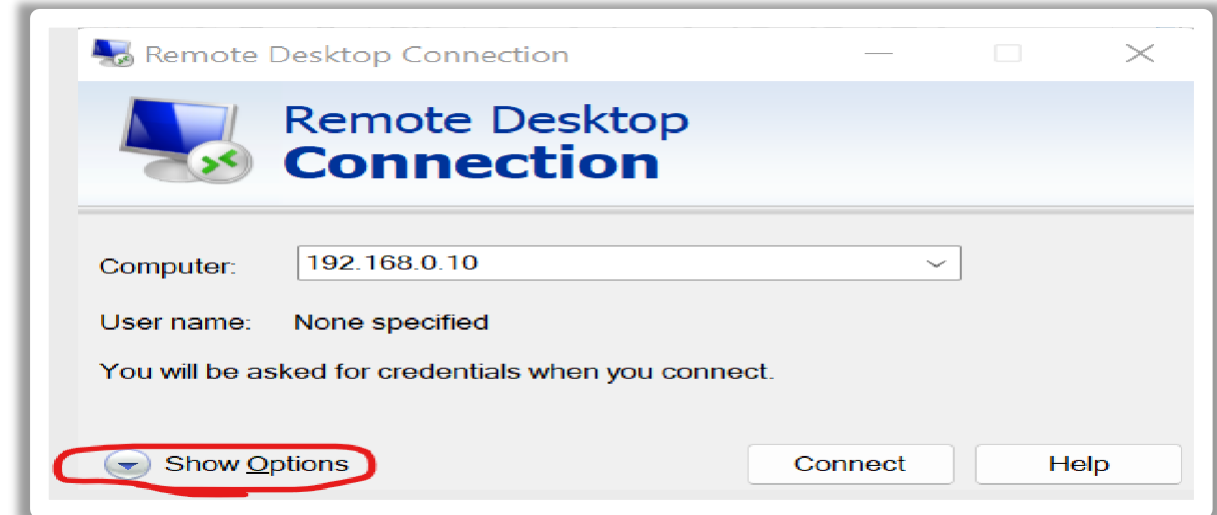


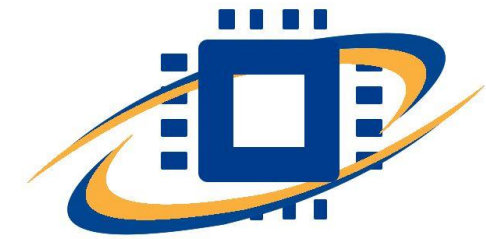
REMOTE DESKTOP CONNECTION

Windows Machine:

open the **Remote Desktop Connection** application and follow the below steps to connect to the server.

- Enter the server address as **192.168.0.10**
- Click on show options, go to Display tab and change the **High color (32 bit)** to **High color (16 bit)**
- Click on **Connect**
- This would launch **VNC Client** login window as shown in next slide.

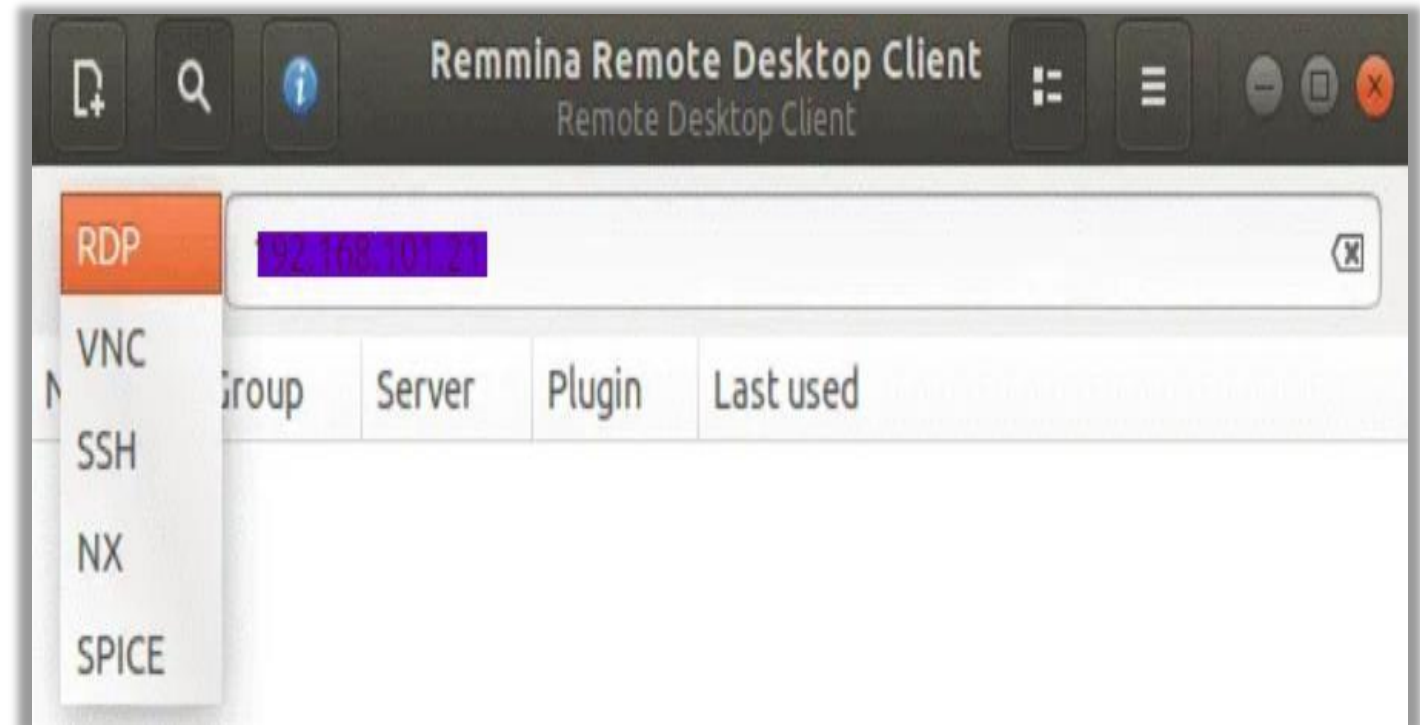




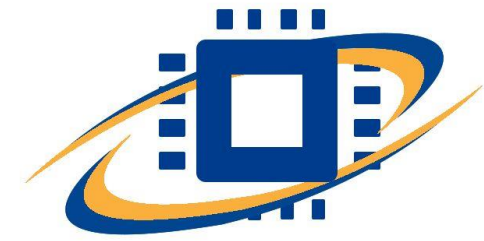
REMMINA REMOTE DESKTOP CLIENT

Linux machine:

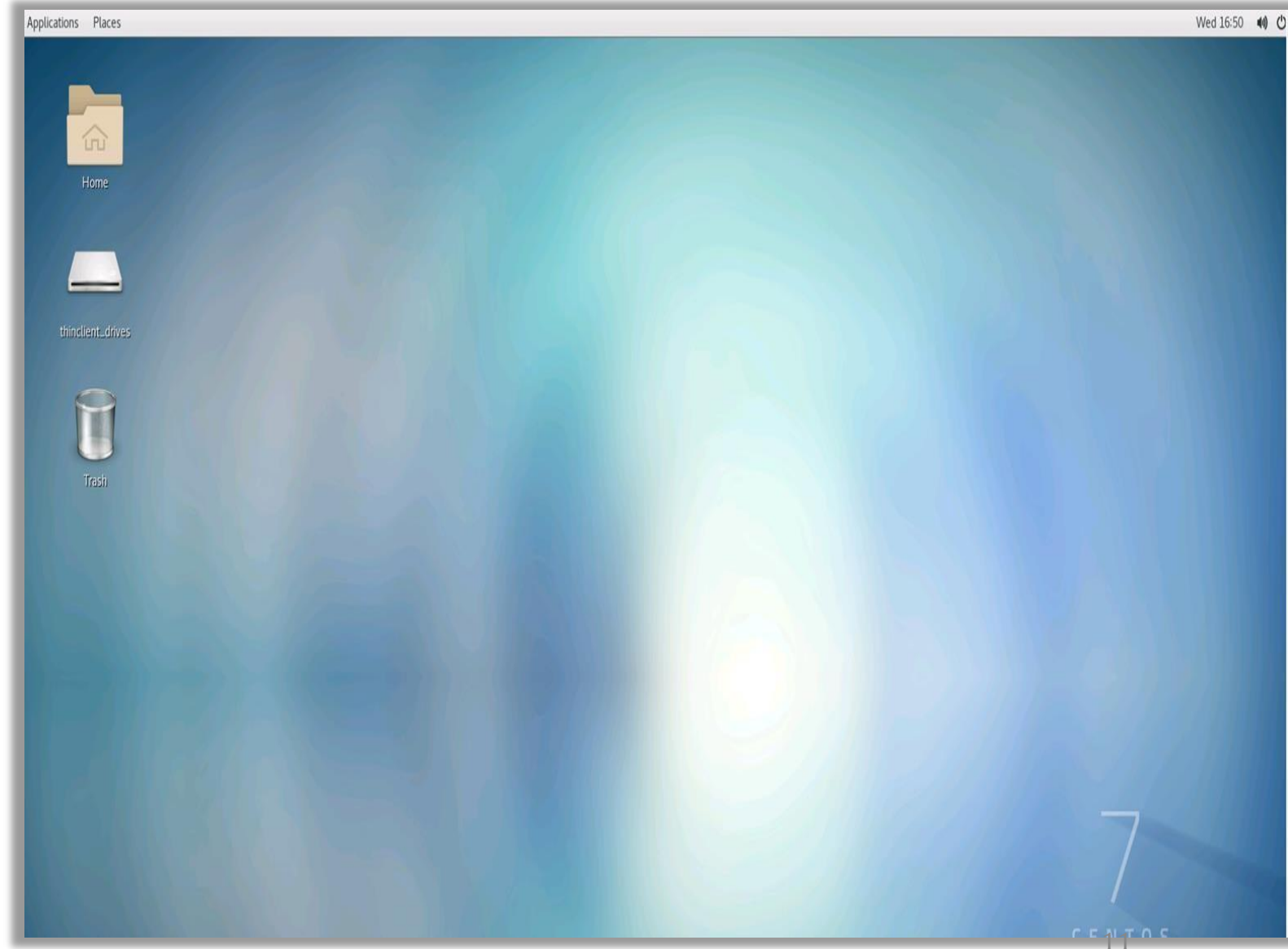
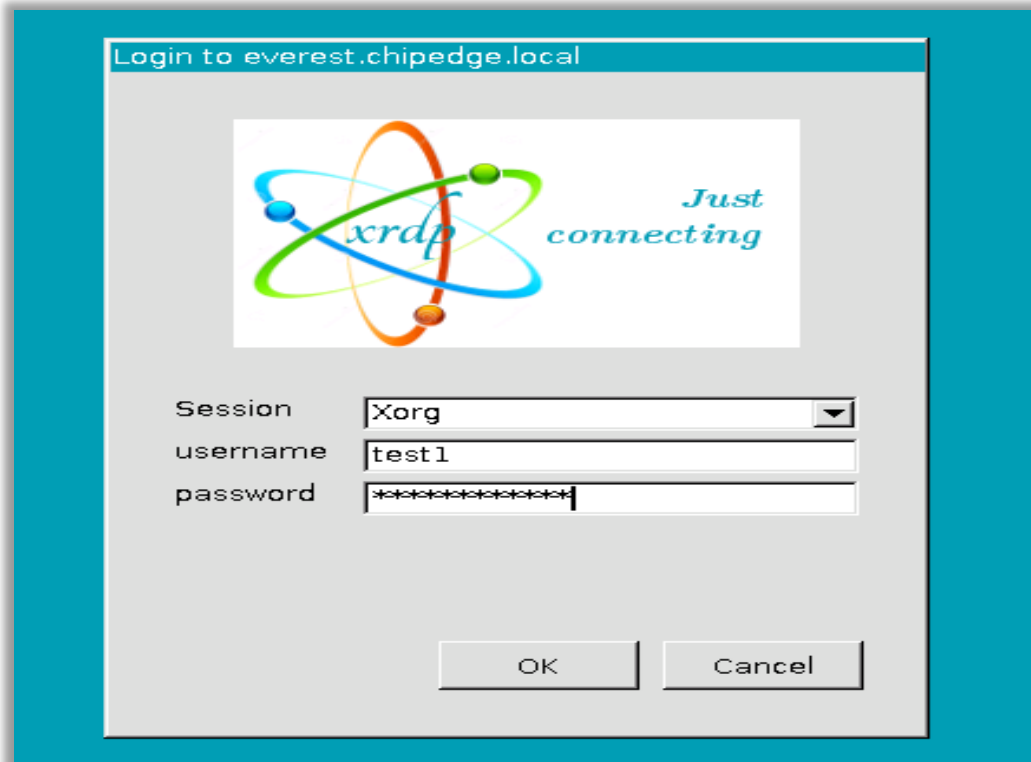
- In the opened Remmina window, select **RDP** in the drop-down list
- Enter the IP address of the remote host (192.168.0.10 in this case) and hit **Enter**

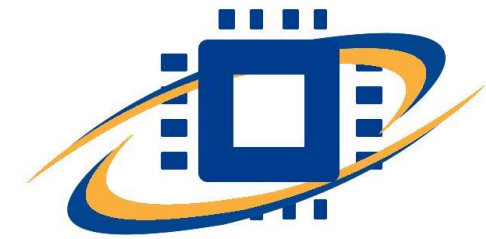


REMOTE DESKTOP CONNECTION



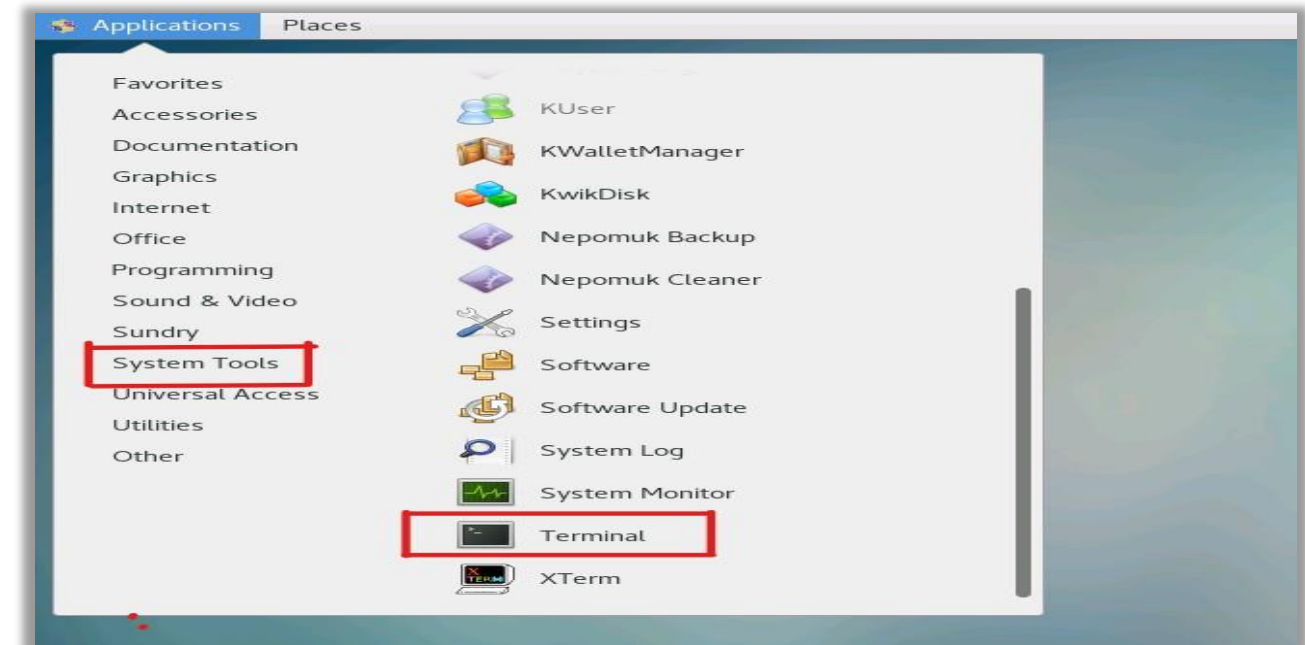
- Enter the **server** login credentials as provided to you.
- Linux Desktop View after login to the server



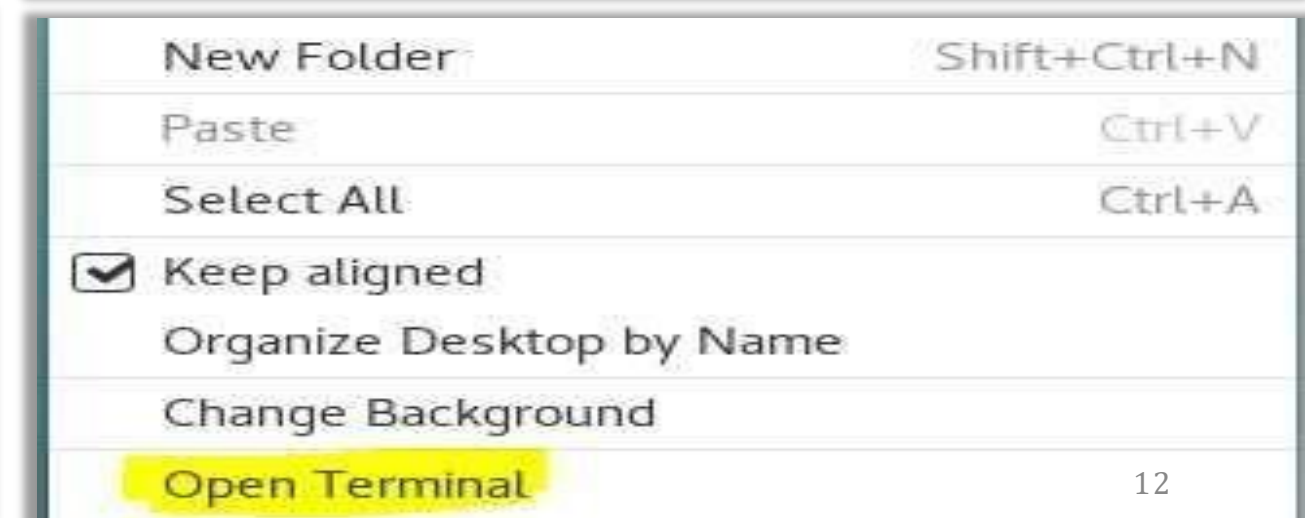


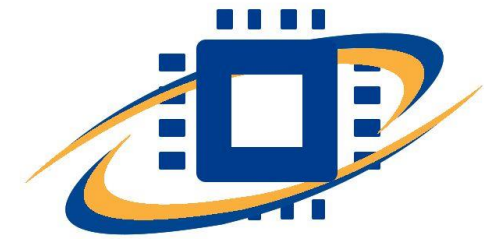
Once you login to the server open terminal

- Click on **Applications >> System Tools >> Terminal** or **Right click** on the desktop and click on **open terminal**
- A terminal will be opened for your inputs



```
test1@kailash:~  
File Edit View Search Terminal Help  
[test1@kailash ~]$ pwd  
/home/test1  
[test1@kailash ~]$ █
```





PASSWORD CHANGE

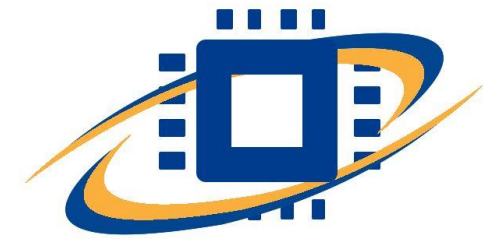
It is highly recommended to change the server password.

- In terminal run the command **passwd**
- enter your current UNIX password as provided to you
- enter new password
- confirm the new password
- you will see a message that tokens updated successfully

Please note that the password which you are entering is not visible on the Unix terminal, just type the password as it is and hit the enter button.

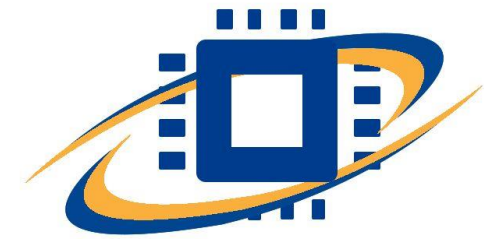
And note down the password in some place for future use.

```
File Edit View Search Terminal Help
[test1@everest ~]$ passwd
Changing password for user test1.
Changing password for test1.
(current) UNIX password:
New password:
Retype new password:
passwd: all authentication tokens updated successfully.
[test1@everest ~]$
```



USAGE LIMITS & OTHER DETAILS

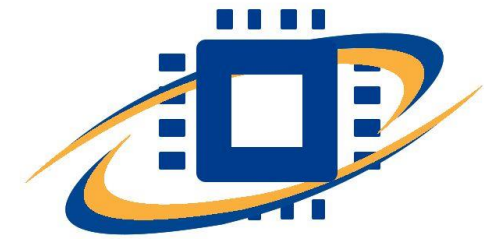
- Users are allocated with default work hour for a day and week.
- Week starts on Monday morning (12.01AM) and ends Sunday night (12.00AM). It's up to you to use this quota allocated to you within the week
- Users can check their current week and day usage
- User's sessions will get auto killed after 30 minutes if the session are idle or disconnected
- Maximum of 50 Unused hours get added to the next week
- If he/she crossed these limits, his/her account will be **locked** till next Monday or for a day and **you will see an access denied message**, so please follow the recommendations to avoid unnecessary inconvenience.



USAGE MANAGEMENT

- Usage count starts the time when user login to the server
- Users can check their current week and day usage by running the below command on your Linux terminal
- Command to check the usage: **sessctl status**
- Introducing new carry forward feature. Maximum of **50 unused hours** would be automatically adding to next week for all the users.

```
[test1@kailash ~]$ sessctl status  
  
still your today's session haven't been calculated.  
  
Today's allowed mins: 480, utilised: 0  
Week's allowed mins: 3000, utilised: 0  
  
[test1@kailash ~]$ █
```



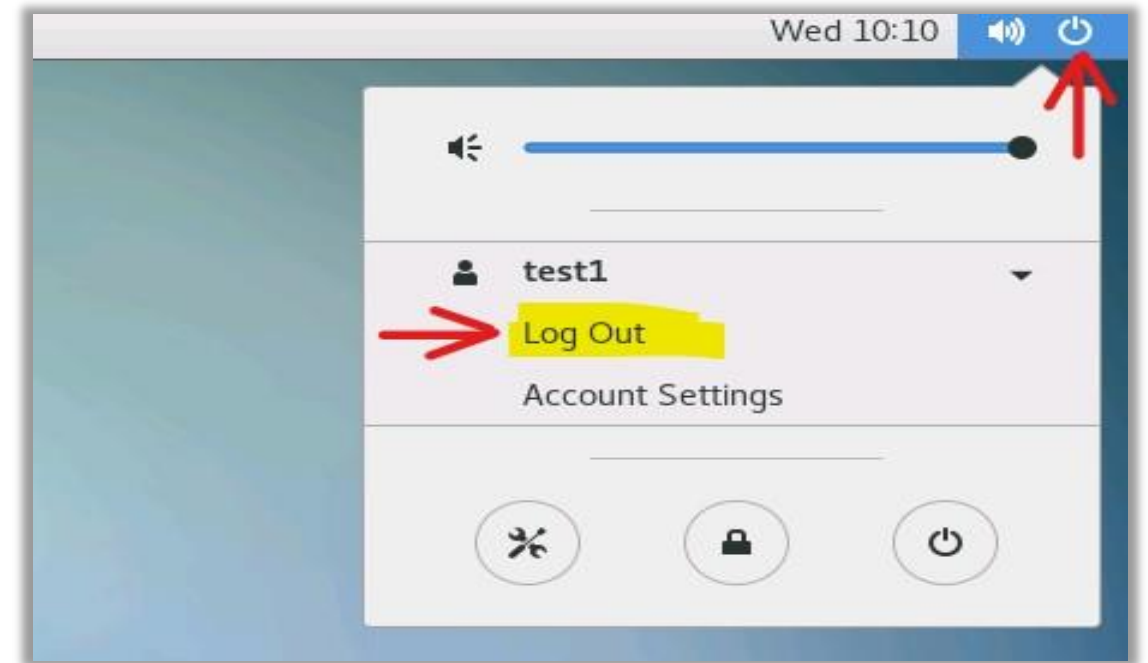
LOGOUT THE RDC (remote desktop connection)

It is mandatory to logout from the server after the lab practice than leaving it.

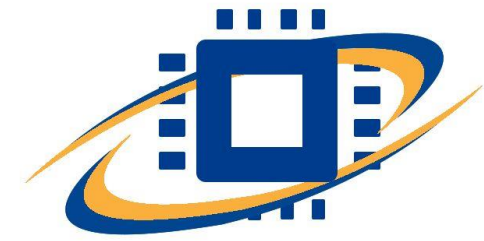
Please note if you do not log out, the session would be running in background and your usage is counted.

TO LOGOUT

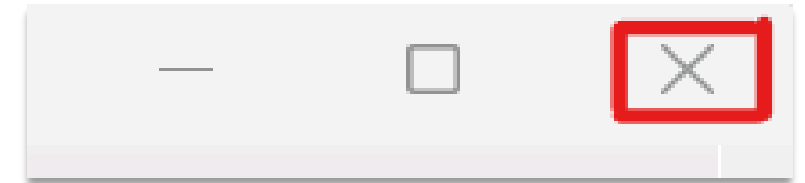
Click on the **power icon** at top right corner >>
Drop down arrow >> Logout

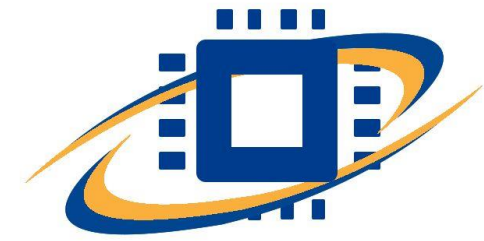


DON'Ts



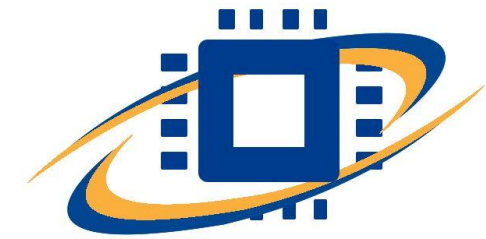
- After your lab work is done, Do not close the remote desktop connection (RDC) session using X button as show below. But logout properly as mentioned above
- Do not disconnect the VPN without logging out from the server
- In both the scenarios if the sessions are closed or disconnected without logout, your session would be running in background. Hence the system will consider that you are still logged in and count the usage until the session got auto killed
- Do not keep the default Unix password (password shared by the Chipedge IT) unchanged





DO's

- Change your default server password once in a month
- Check your usage frequently or as needed
- Logout from the remote desktop connection (RDC) application immediately after your lab practice
- Disconnect the VPN after logout from the RDC



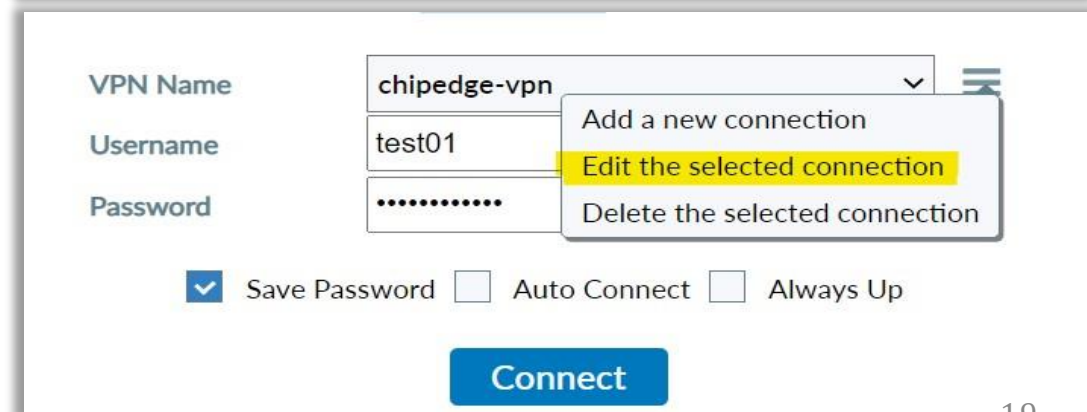
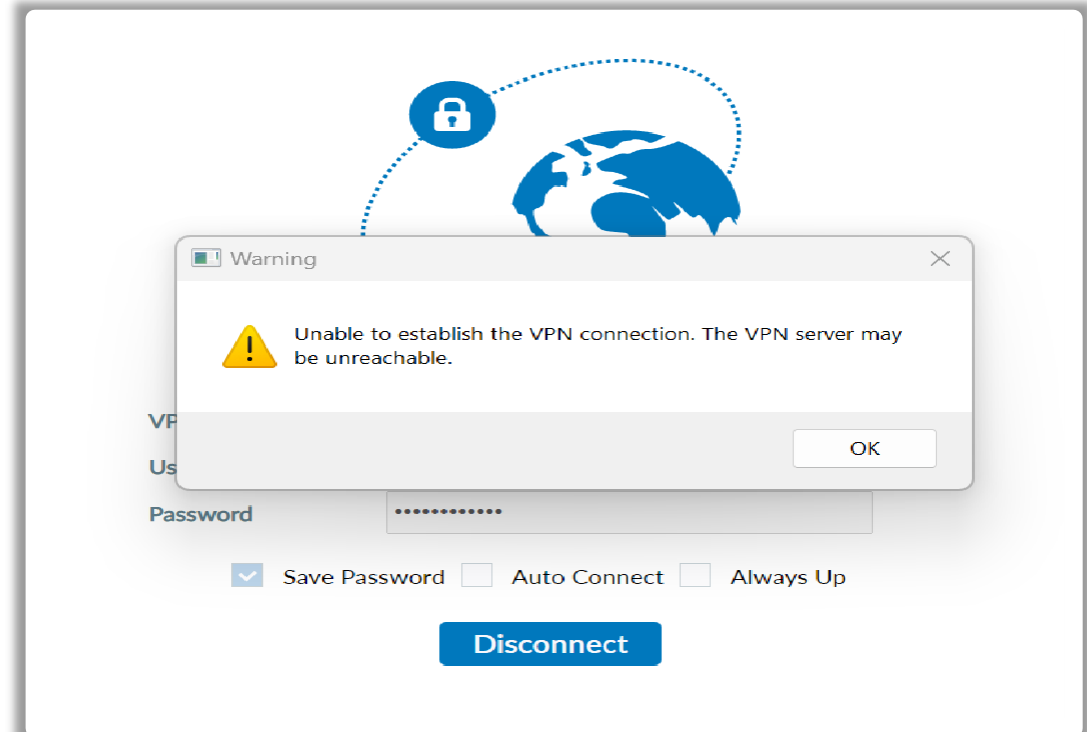
COMMON ERRORS AND HOW TO FIX IT

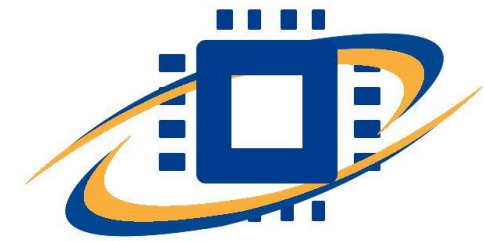
Problem:

Unable to establish the VPN connection. The VPN server may be unreachable

How to fix it?

- Check the VPN configuration setting, if all the settings are properly saved
- Click on the **3 lines** next to the VPN name **Edit the selected connection >>** check all the settings are saved as image shown in the next slide





COMMON ERRORS AND HOW TO FIX IT...contd

- If the settings are not saved as per the image, please change the settings accordingly and save
- Connect to the VPN after rechecking all the settings are properly saved.
- If the issue persists, contact Chipedge IT support

Edit VPN Connection

VPN: **SSL-VPN** | IPsec VPN | XML

Connection Name:

Description:

Remote Gateway: ✕
[+Add Remote Gateway](#)

☒ Customize port

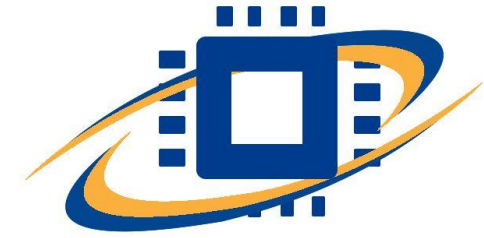
☐ Enable Single Sign On (SSO) for VPN Tunnel

Client Certificate: ▼

Authentication: ☒ Prompt on login ☐ Save login
☐ Enable Dual-stack IPv4/IPv6 address

Cancel **Save**

COMMON ERRORS AND HOW TO FIX IT...contd

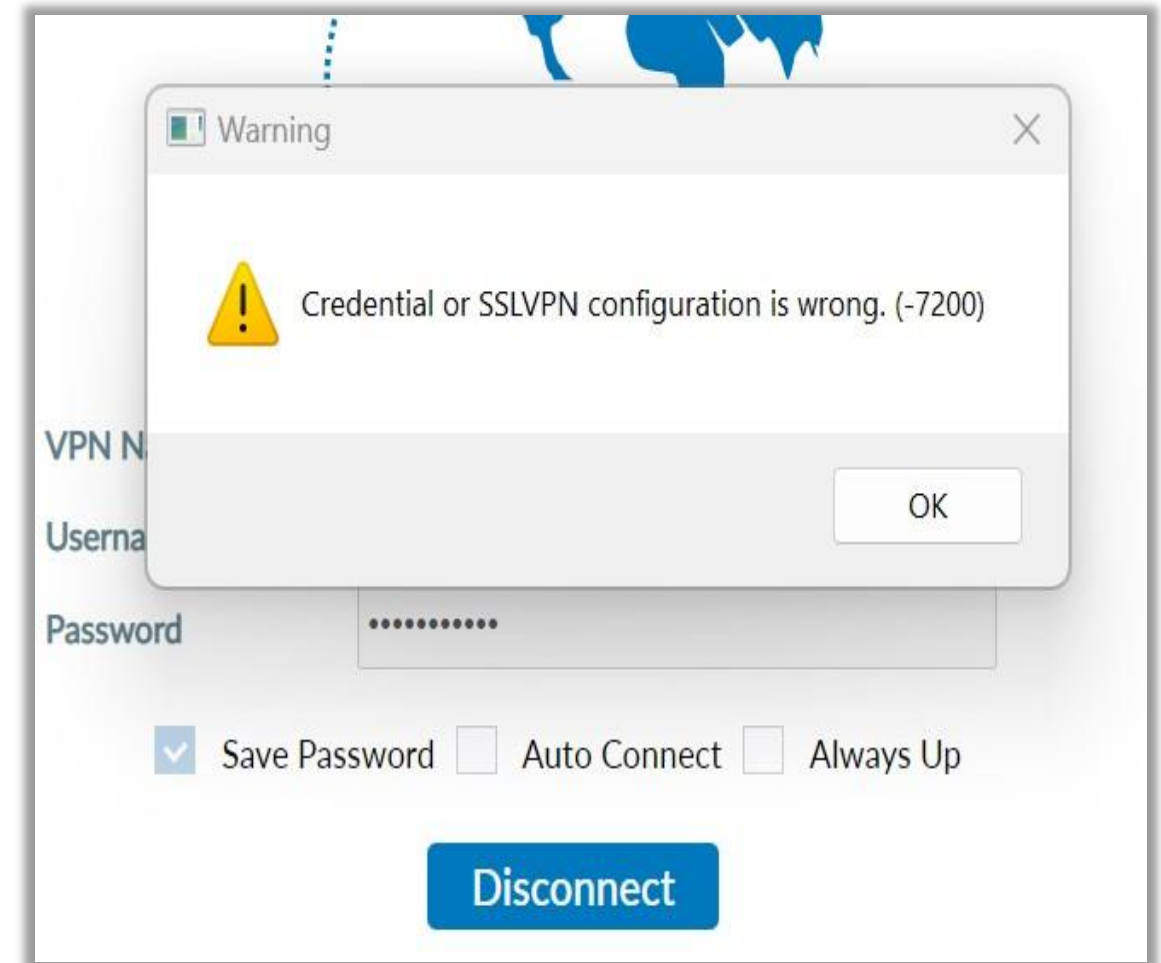


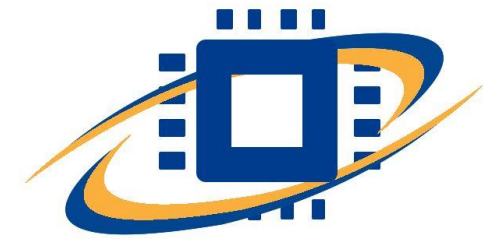
Problem:

**Credential or SSLVPN configuration is wrong.
(-7200)**

How to fix it?

Recheck the credential are entered correctly or not. If the provided credential is correct and the problem persist, there might be issue with your ID level, hence contact the Chipedge IT support.





COMMON ERRORS AND HOW TO FIX IT...contd

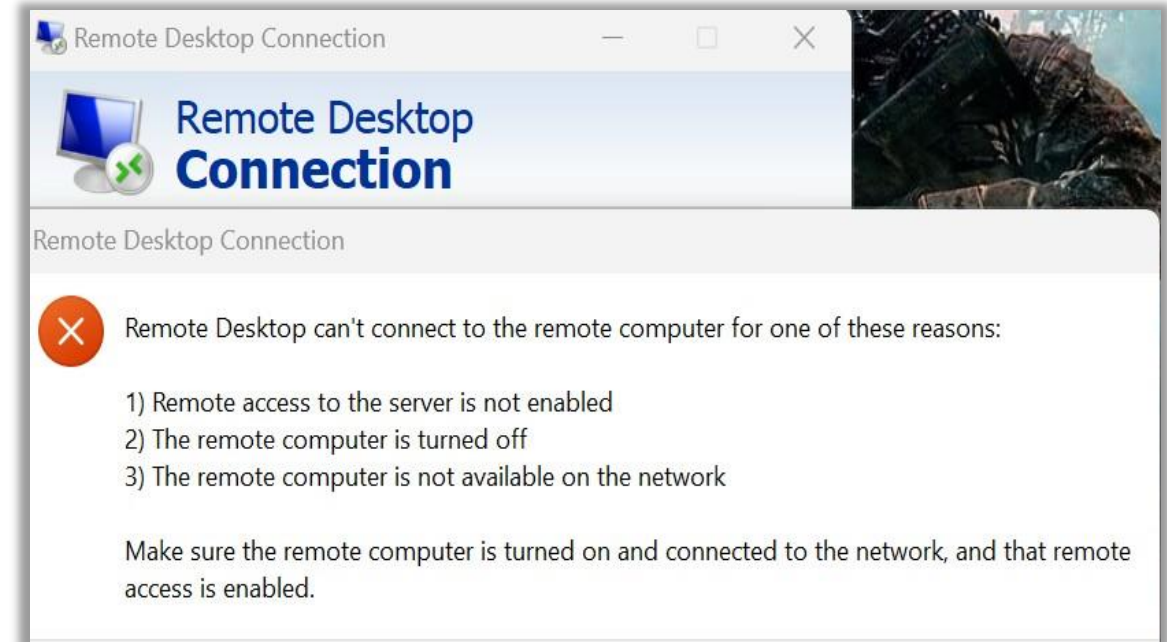
Problem:

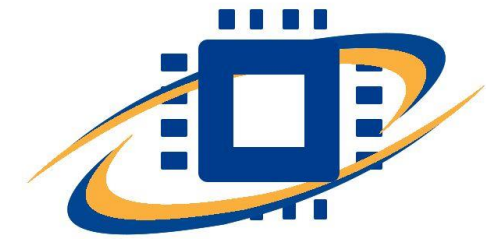
Remote desktop can't connect to the remote computer for one of these reasons:

How to fix it?

This problem is because you are not connected the Chipedge VPN. Connect to the Chipedge VPN (Forticlient VPN) and reconnect the RDC

If the issue persist even after the VPN is connected, contact Chipedge IT support





COMMON ERRORS AND HOW TO FIX IT...contd

Problem

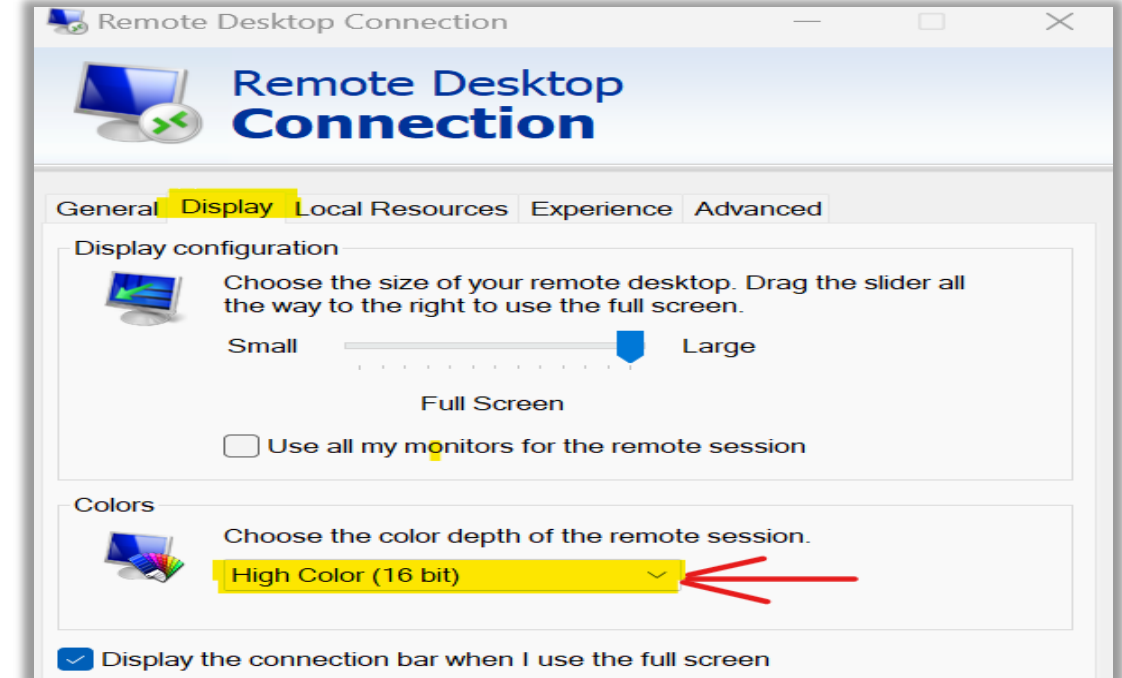
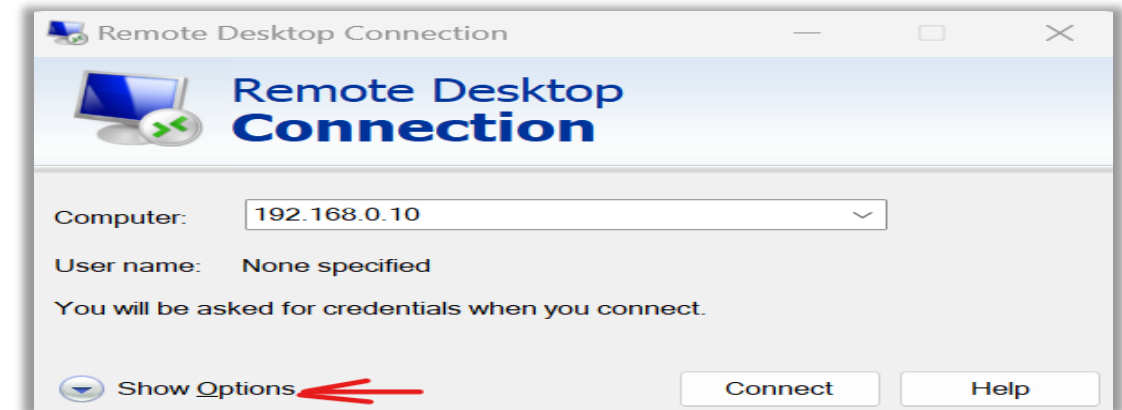
RDC is lagging, To open a terminal or when typing it is taking longer than expected time

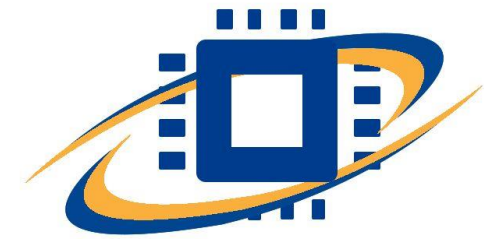
How to fix it?

Check the display setting in RDC, follow the below steps to check the display

Open **RDC** >> click on **show options** >> Go to **Display tab** >> Choose the color depth **High color (16 bit)**

If the issue persist, check your internet bandwidth basically the RDC needed 60 to 100 MBPS bandwidth





COMMON ERRORS AND HOW TO FIX IT...contd

Check your internet connectivity by pinging to chipedge server

Open Windows/Unix command prompt and run the below command on the terminal

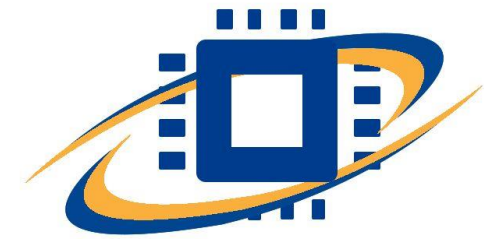
Command: **ping 180.179.249.110**

Time Latency should be less than **20ms** for smooth GUI operation

```
C:\Users\itadmin_chipedge>ping 180.179.249.110

Pinging 180.179.249.110 with 32 bytes of data:
Reply from 180.179.249.110: bytes=32 time=9ms TTL=247
Reply from 180.179.249.110: bytes=32 time=9ms TTL=247
Reply from 180.179.249.110: bytes=32 time=9ms TTL=247
Reply from 180.179.249.110: bytes=32 time=20ms TTL=247

Ping statistics for 180.179.249.110:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 9ms, Maximum = 20ms, Average = 11ms
```

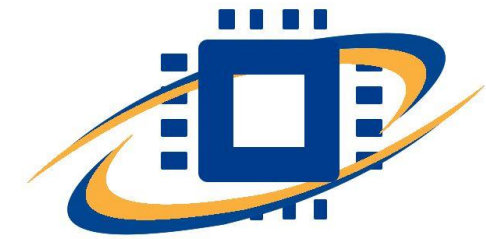
IT HELPDESK

If Your issues are not fixed by above solutions, Please file a ticket by sending an email to "**training@siliconchip.in**" from your registered email address with following details.

- Server username:
- VPN username:
- Mobile number :
- Problem description :
- Snapshot to understand the problem (Preferable)

It is mandatory that users must raise ticket for any IT issues. After sending email, If the IT admin do not revert in 30 minutes, please call the IT support number:

- Support No: +
- Name : Mr. Support Hours : 9 AM to 9 PM



ESCALATION MATRIX

If the IT support didn't revert on your ticket and phone is not connecting or you didn't satisfactory solution for your issue, please escalate to next level.

Primary Contact	First level escalation	Second level escalation
Akash Kumar - IT Admin	Kousalya S – Learning Experience Manager	Prasad Joshi – C O O
<u>support@chippedge.com</u> 91488 20446	<u>Kousalya@chippedge.com</u> 76248 23338	<u>prasad@chippedge.com</u> 96117 21778