Accessing the
IBM Technology Zone

v8.0
last updated by ADL 5/7/2024

NOTE: IF YOU ARE AN IBMer EITHER AT AN IBM LOCATION OR CONNECTED TO IBM FROM A HOME OR REMOTE OFFICE YOU DO NOT NEED TO USE THIS GUIDE.YOU ALREADY HAVE ACCESS TO THE SYSTEMS FROM THE IBM INTRANET.

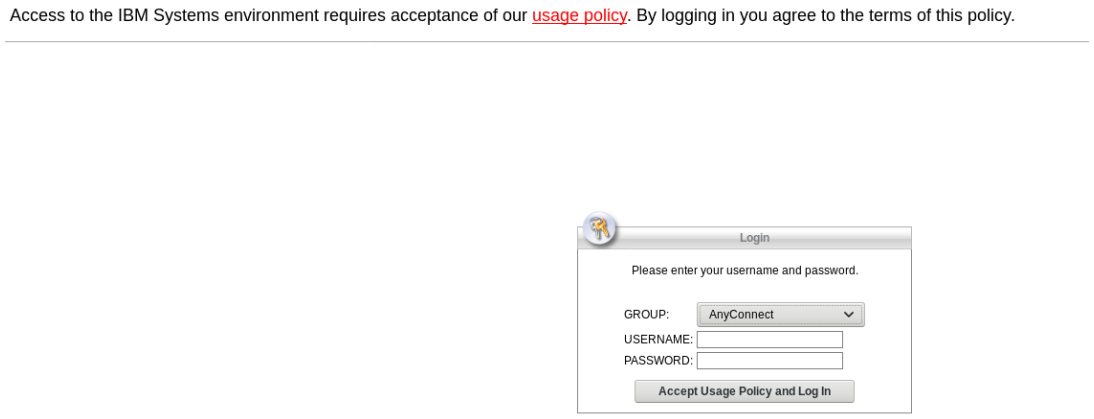
Section 1 : VPN Portal

This is the easiest and most common method for gaining access to the IBM Technology Zone, and is the one you will use unless the project manager has instructed otherwise. Access to the portal requires a browser with Java enabled. Windows, Mac, and Linux are supported, but see Appendix A for full details on system requirements.

Note: Every OS and browser has their own look, security policy, and notification system. What follows is an example connection using Windows 7 and Firefox. You may see more “pop-ups” or perhaps none at all, but it is important to follow the messages that do appear, so that the installation process is not blocked or disabled.

Open your browser and enter https://asa003b.centers.ihost.com in the address field. If for some reason the name is not resolving, you can use the IP address (131.239.211.196). The URL will automatically expand to the one shown in the following screenshot:

NOTE: IF YOU ALREADY HAVE CISCO ANYCONNECT 4.10 OR GREATER INSTALLED ON YOUR SYSTEM YOU SHOULD SKIP TO SECTION 3 – Connecting the VPN

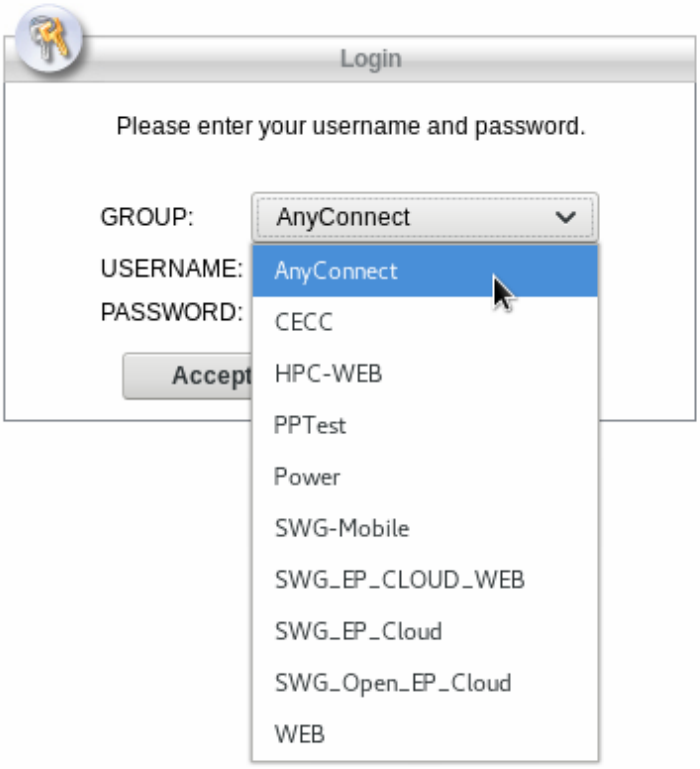


You will be presented with the welcome screen shown above. If you do not see it, if the page does not load, there are some things to check:

1. Do you have a firewall installed on your system that may be blocking the connection?
2. Is your browser configured with a proxy that restricts access to certain sites?
3. Are you on a corporate network with restricted internet access?

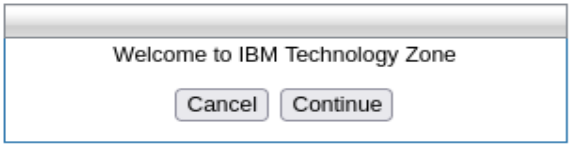
You may need to engage your local IT helpdesk to help resolve the connectivity issues.

Assuming the page loads properly, in the middle of the screen you will see the Login section. The Group is a drop-down menu, but unless told otherwise by the project manager, you should choose the default **AnyConnect**.



Then, enter the VPN username and password assigned to you – if you do not have one, contact your project manager.

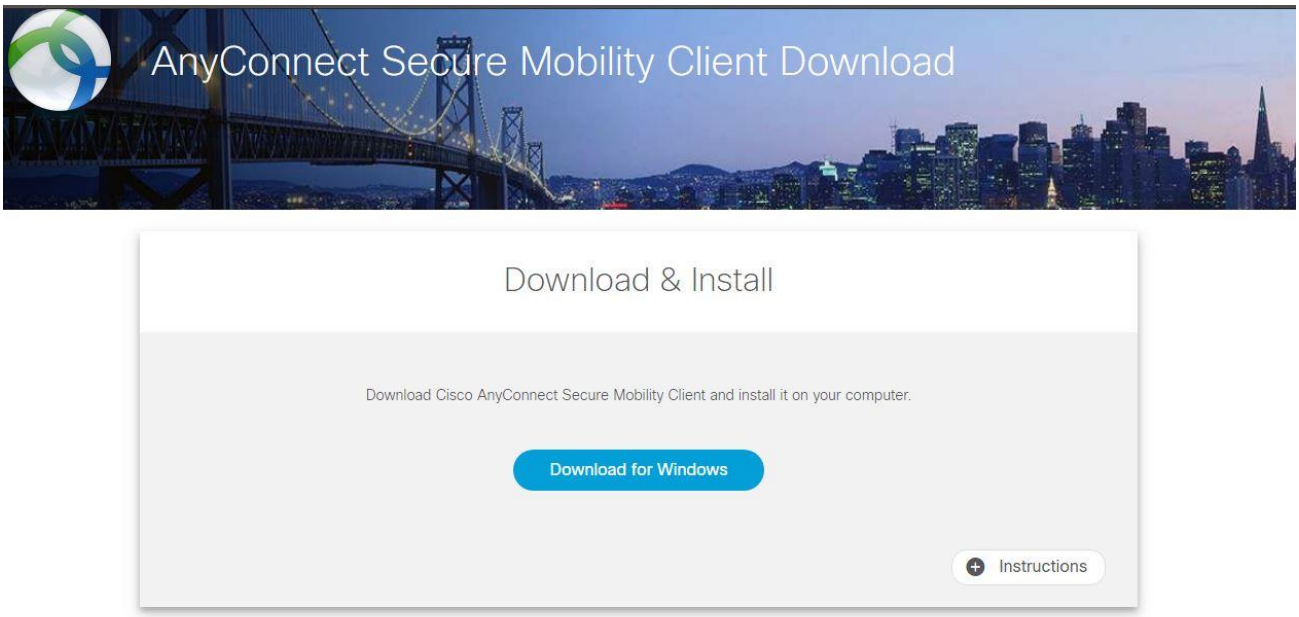
Before clicking “ACCEPT Usage Policy AND Log in” please read and understand the usage policy accessible via the link at the top of the log in page.



If the authentication succeeded, you will see a welcome screen (exact wording may differ depending on your group selection).

If authentication did not succeed, you will see a “Login Failed” message. Verify the password and try again, and if it still does not work, contact your project manager.

Once you click 'Continue', the download and install process will begin. You will be presented with the following screen which will be tailored to your operating system.



Click on the Download button to begin downloading the client installer. Save the file to a known location for easy access.

Once the download completes, browse to the location of the saved file and open, run, or execute the file as required by your OS.

This will attempt to install the VPN client. During this process you may see various warning messages from the browser, from anti-virus application, or from the OS itself (password requested for installing new software, etc). In all cases, it is important to be aware of what the messages say.

Choose appropriate selections that will allow the install to continue.

Section 2 : Manual VPN installation

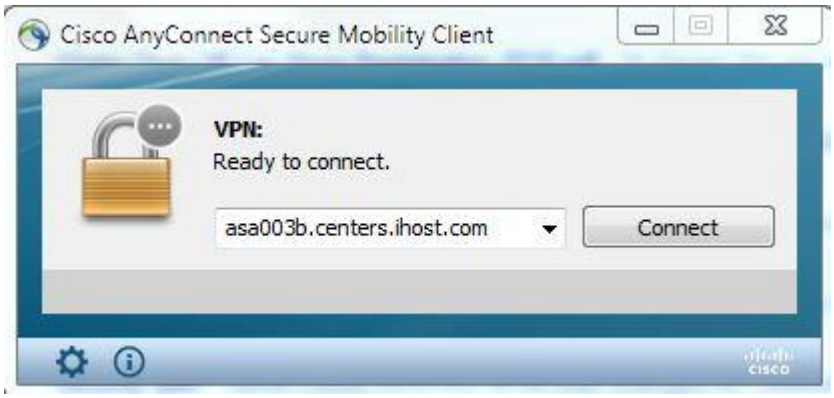
Occasionally you may experience difficulty with the automatic download process, in which case a manual install of the client may be necessary. If this situation occurs please contact you IBM project manager who is able to provide a URL from which to download the standalone client installer.

Once obtained, run the installer to install the Anyconnect client.

Section 3 : Connecting the VPN

At this point you have the client installed; if the installation did not work for you, please contact the project manager, as alternative access measures will have to be implemented.

To log into the IBM Technology Zone, start the client, enter **asa003b.centers.ihost.com** in the box and click connect. When prompted choose AnyConnect as the group (unless told otherwise), and enter the VPN id and password the project manager assigned to you.

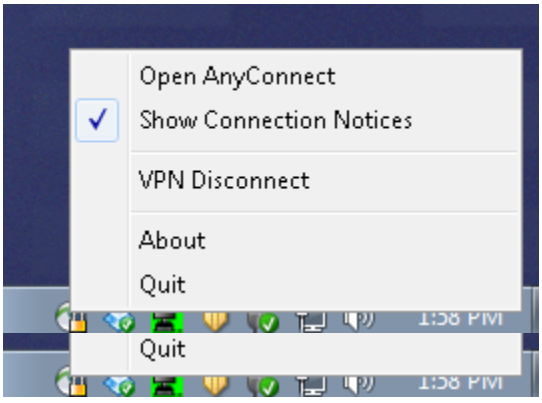


Users on Linux may see an initial warning message saying the server is untrusted. This is a known bug, and is not accurate (the gateway does use an SSL certificate from a known and trusted CA). If this happens to you, please select 'Connect Anyway' and then enter the information as mentioned above.

If your connection to the gateway fails please contact the project manager, who will engage the technical team to help debug the issue and possibly recommend alternative access if the issue cannot be resolved.

If the connection is successful, you will see the VPN client icon in your system tray (or equivalent)

Right-clicking the icon will bring up a menu where you can see more details or disconnect/quit your session.



Congratulations, you are now able to access the resources assigned and provided to you by the project manager. See Section 4 if you'd like steps to help verify that your connection is working.

Section 4 : Verifying connectivity & Troubleshooting

It Looks Good But How Can I Be Sure?

This one is easy – attempt to access the server(s) assigned to you by the project manager (and listed in the turnover documentation). The simplest method is to ping the server (by name or IP) – since the servers are not reachable directly from the internet, but only from a valid VPN connection. A successful ping means you are connected to the IBM Technology Zone, and you can begin your project.

Bad Ping (as performed from a Linux workstation):

For Example: The IP below is for the purpose of this example only and your test should be performed to an IP address listed in the turnover doc provided to you by your project manager.

```
$ ping 129.40.2.102

PING 129.40.2.102 (129.40.2.102) 56(84) bytes of data.
^C
--- 129.40.2.102 ping statistics ---
3 packets transmitted, 0 received, 100% packet loss, time 2275ms
```

Good Ping:

```
$ ping 129.40.2.101
PING 129.40.2.101 (129.40.2.101) 56(84) bytes of data.
64 bytes from 129.40.2.101: icmp_seq=1 ttl=121 time=2.33 ms
64 bytes from 129.40.2.101: icmp_seq=2 ttl=121 time=1.20 ms
64 bytes from 129.40.2.101: icmp_seq=3 ttl=121 time=1.08 ms
^C
--- 129.40.2.101 ping statistics ---
3 packets transmitted, 3 received, 0% packet loss, time 2261ms
rtt min/avg/max/mdev = 1.081/1.540/2.331/0.561 ms
```

If you were assigned multiple servers, but only some of them are reachable, it is possible that others in your group are already on them, and have rebooted or otherwise took them offline for some reason. But if that isn't the case, contact the project manager who will engage the technical team to investigate.

It Doesn't Look Good But How Can I Find Out the Problem?

Scenario 1: VPN does not connect; install fails
Send the following information to the project manager (more detail is better):
1. OS (for example, Windows 7 or Redhat 6.3)
2. Browser type and version (if using the web portal)
3. Screenshot(s) showing the error condition

Some common reasons for this error:

* Having another VPN active (disconnect and retry)
* Blocked by firewall/AV software (temporarily disable and retry)

Scenario 2: VPN appears to connect, cannot reach servers
If the VPN client shows that it is connected, but none of the servers assigned to you are reachable (ping fails), send the following information to the project manager:

1. Output of interface information. On Windows, open a command prompt and type “ipconfig”. On Linux and MAC, open a terminal and type “ifconfig”. You should see an interface in the 129.40.x.x network, which is the IP range used by the IBM Technology Zone.
2. Output of your system's routing table. On Windows, open a command prompt and type “route print”. On Linux and MAC, open a terminal and type “netstat -r -n”.

Scenario 3: VPN connects, ping to server works, but application does not.
The VPN policy does not restrict access to specific ports (if you are allowed to access a server, you are allowed full access to the server), but it is possible the application is not active, or not listening on the public interface. Contact the project manager, who will engage the technical team to determine the application state. If SSH is working, then you should be able to check this out as well (on Linux) by running “netstat -tuap” to see all the listening ports.

If you are still having problems accessing the environment, contact the project manager, providing as much detail as possible to help the technical team determine and resolve the problem.

Section 5 : Changing your VPN password

Once connected to the IBM Technology Zone, open your browser to:
https://ccad2.pbm.ihost.com/ssp/index.php (click Accept or Yes or Proceed if prompted, as the site uses a self-signed certificate). Fill out the fields and click Change Password.

Appendix A : System Requirements

Current VPN client version is 4.9.06037; requirements that follow are adapted from the VPN client release notes.

Microsoft Windows

Supported Versions:
Windows 7 SP1 x86 (32-bit) and x64 (64-bit)
Windows 10 (32-bit) and x64 (64-bit)
Windows 11 (32-bit) and x64 (64-bit)

Notes:
Windows 2008 is not officially supported, but it is possible to install the client on this OS
To start AnyConnect with WebLaunch, you must use the 32-bit version of Firefox 3.0+ and enable ActiveX or install Sun JRE 1.4+.
Internet Explorer 6.0 is no longer supported

Linux

Supported Versions:
Red Hat Enterprise Linux 6, 7 and *8*
Ubuntu 12.04(LTS), 14.04 (LTS) and 16.04 (LTS) 64-bit only
Notes:
Superuser privileges are required for installation
Java 5 (1.5) or later. The only version that works for web installation is Sun Java. You must install Sun Java and configure your browser to use that instead of the default package.

Mac OS X

Supported Versions:
Mac OS X 10.10, 10.11, & 10.12
Notes:
Mac OS X 10.8 introduced a new feature called Gatekeeper that restricts which applications are allowed to run on the system. You can choose to permit applications downloaded from:

- Mac App Store
- Mac App Store and identified developers
- Anywhere

The default setting is Mac App Store and identified developers (signed applications). AnyConnect release 4.4 is a signed application, but it is not signed using an Apple certificate. This means that you must either select the *Anywhere* setting or use Control-click to bypass the selected setting to install and run AnyConnect from a pre-deploy installation. Users who web deploy or who already have AnyConnect installed are not impacted. For further information see:
http://www.apple.com/macosx/mountain-lion/security.html .

Appendix B : Linux manual install process

The manual install file for Linux requires some additional steps, which are:

1. Download the file (see Section 2 for details)
2. Open a terminal window and become root user (su)
3. Change to the directory where the file is located (cd)
4. Decompress the file (gzip -d <filename>)
5 Untar the file (tar -xvf <filename>). This creates a new directory called anyconnect-<version>.
6. Enter the new directory (cd anyconnect-<version>)
7. Change to the vpn subdirectory (cd vpn)
8. Run the command to install the client (./vpn_install.sh)
9. Follow the prompts (accept the license agreement)
10. When install completes, the client will be located in **/opt/cisco/anyconnect/bin**, although if you are using a graphical window program (like Gnome), it should more easily be found under Applications – Internet. Run the client (file name is **vpnui**) and follow the same access procedure as listed in Section 2.