|  |
| --- |
| cid:image001.png@01D11266.F12EB7F0  HPE NonStop Advanced Technology Center  Remote Access User’s Guide |
|  |  |

# Table of Contents

Notice...........................................................................................................................3

Welcome.......................................................................................................................4

Overview of SSL/VPN…….............................................................................................4

Service availability.........................................................................................................4

Local Client Remote Access Method……………………………………….…………………….5

OS / Browser Compatibility............................................................................................6

Admin rights……………………………………………………………………………………...7

Trusted Sites………………………………………………………………………………...……9

Go to the Remote Access page........................................................................................9

Login Status.................................................................................................................12

Terminate the SSL/VPN Tunnels.....................................................................................14

Appendix A - How to check for 32-bit browser in IE…….…………….……….……………15

Appendix B – Manually Installing Browser Addon /Plugin…………..……….….….………16

Appendix B - How to Remove SSL/VPN Components……………..…………….….……….16

Notice

Legal Notices

Copyright

Copyright 2013, F5 Networks, Inc. All rights reserved.

F5 Networks, Inc. (F5) believes the information it furnishes to be accurate and reliable. However, F5 assumes no responsibility for the use of this information, nor any infringement of patents or other rights of third parties which may result from its use. No license is granted by implication or otherwise under any patent, copyright, or other intellectual property right of F5 except as specifically described by applicable user licenses. F5 reserves the right to change specifications at any time without notice.

F5, BIGIP are trademarks of F5 Corporation in the U.S. and other countries.

Microsoft, Windows, and Internet Explorer are trademarks of Microsoft Corporation in the U.S. and other countries.

Hewlett-Packard Enterprise Company shall not be liable for technical or editorial errors or omissions contained herein. The information in this document is provided “as is” without warranty of any kind and is subject to change without notice. The warranties for HP products are set forth in the express limited warranty statements accompanying such products. Nothing herein should be construed as constituting an additional warranty.

Welcome

Dear HPE NonStop ATC Remote Access User,

Welcome to the HPE’s NonStop Advanced Technology Center (ATC). The HPE NonStop Advanced Technology Lab (ATLab) is located inside the NonStop Advanced Technology Center (ATC) and is managed by the ATC Operations group. The ATC Operations group manages all computer and network resources in the Advanced Technology Lab (ATLab). This guide documents the SSL/VPN remote access method into the ATLab Network. This guide is designed to assist you with your remote access and walk you through the process of successfully connecting to your designated resources in the ATLab. We have provided this service to you for your convenience during the timeframe the HPE NonStop ATC resources are booked for you.

HPE NonStop ATC currently offers a SSL/VPN remote access method into the ATLab.

Service Availability

This service is available 7x24x365 for remote users to gain access into the ATLab. The ATC operations group will assist users with remote access issues between the hours of 07:00 and 17:00 PST Monday - Friday.

### Overview of SSL/VPN

There are two SSL / VPN remote access methods to access the Advanced Technology Lob (ATLab). One method is browser based and the other is client based that is pre-configured and installed on the ATLab user’s computer. The remote Access client method is required for Firefox 44 and newer and Chrome 40 or newer users. Both of the newer Firefox and Chrome browses no longer support the Mozilla plug-ins. Both methods provide a secure 2048-bit encrypted tunnel into the ATLab. Each remote access method is detailed in this document.

Local Client Remote Access Method

Remote Access clients are available for both Windows and Linux. To download the ATLab Remote Access clientfor both OS’s ftp to the ATLab ftp server and logon as the ftp-f5 user and follow this ftp command line procedure:

ftp [ftp.atc-hpe.com](ftp://ftp.atc-hpe.com)

atc-hp\ftp-f5 (userid)

Welcome01 (Password)

get **bigipedgeclient.exe** (Windows)

get **linux\_sslvpn.tgz** (Linux)

bye

Once the Remote Access client is downloaded the user will need to install it. Simply install the client on the computer that will be used to access the ATLab.

**Windows Local Client Installation**

Once the Remote Client is downloaded the user will need to execute the installer bigipedgeclient.exe. The Remote Client is preconfigured and after it is installed simply start the Remote Client and click on “Connect” for the Remote Client to initiate the SSL connection to the ATLab.

**Installing the CLI for Linux**

Install the command line interface for Linux so that users can start and stop Network Access sessions from the command line.

1. Extract the file linux\_sslvpn.tgz to your local directory.
2. Extract the file linux\_sslvpn.tar to your local directory.
3. Run the install script Install.sh under the root account.

The following text appears when installation is complete:

--> f5fpc is installed in /usr/local/bin

--> Please check f5fpc --help command to get started

--> Uninstaller located in /usr/local/lib/F5Networks/uninstall\_F5.sh

To start the Linux CLI client, issue the following command

f5fpc –host 50.59.187.73 –user <*userid*> --password <*password*> -x

Browser Based SSL/VPN Access Method

Once a NonStop ATC user has obtained his / her username and password they only need to point their browser to <http://atlab.atc-hpe.com> to gain access to their resources. This method supports “Split-Tunneling” allowing the remote user access to their local resources (ex: local printer, file share)

OS / Browser Compatibility

**Microsoft® Windows OS**

F5 Networks supports 32-bit and 64-bit versions Windows® Vista SP2 running IE9, Firefox 34 and older or Chrome 40\*and older and Windows® 7 SP1 and Windows 8.1 Update and Windows 10 running IE11, Firefox 34 and older or Chrome 40\* and older.

* Only 32-bit browsers are supported.
* Microsoft Edge browser is not supported.

**Windows 10 browser support**

* The Windows Internet Explorer browser included in Windows 10 release is supported.
* The BIG-IP APM system does not currently support the Microsoft Edge (Spartan) browser.

IE11 Users: Special note

You must add our website URL to the IE11 Compatibility View Settings. To complete this task, go to: Tools (Gear icon in top right corner) and select Compatibility View Settings. From there add the URL atlab.atc-hpe.com. Only atc-hpe.com will list but this process is necessary in order to use IE11 accessing the ATLab SSL/VPN server.

**Linux Operating Systems**

F5 Networks supports all 32-bit x86 and 64-bit x86\_64 Linux operating systems (OS) with enabled Kernel support for PPP interfaces and libc version 2 or later, running Firefox 43 or Chrome 40\*.

**OS X**

F5 Networks supports Apple® OS X® 10.11, Apple® OS X® 10.10, Apple® OS X® 10.9, Apple® OS X® 10.8, and Apple® OS X® 10.7 devices running Firefox 34, Safari 6.x, Safari 7.x, Safari 8.x, Safari 9.x, or Chrome 40\*. Additional support details for this platform include the following:

* Only manual plugins installation is supported

\* On Chrome versions 34 and above, there is limited feature support due to browser restrictions as mentioned in SOL15326. Only the following clientless features are supported: Portal Access, Citrix and VMware Webtop based launch support. The following clientless features are not supported: End Point Security checks, Protected Workspace, Network Access, MS RDP, Static AppTunnels, Dynamic Optimized AppTunnels, Java RDP, and Java AppTunnels.

**Android**

F5 Networks supports Android™ versions 4 to 5.

For Network Access functionality, please install F5 BIG-IP Edge Client from Google Play. Customers running Android 4.0 or later should install Android EDGE Client for Android 4.x. Also, for secure mobile access to enterprise web applications F5 provides BIG-IP Edge Portal, which can also be downloaded from Google Play.

**iOS**

F5 Networks supports Apple® iOS® versions 6, 7, 8, and 9. For Network Access functionality please install F5 BIG-IP Edge Client from iTunes. Also, for secure mobile access to enterprise web applications F5 provides BIG-IP Edge Portal, which can also be downloaded from iTunes.

* Apple® iOS® 9 is supported

**Windows RT and Phone**

Windows RT and Windows Phone 8 are supported with clientless features (Portal Access, Java RDP, Java AppTunnels, Citrix and VMware Webtop-based launch). Internet Explorer supports Portal Access and Webtop features. Please note the following exceptions:

* Applications tunnels and MSRDP Terminal Services are not supported on these platforms. Windows RT supports Network Access through Inbox F5 VPN Client. Windows 8.1 supports Network Access using BIG-IP Edge Client Windows 8.1, avaiable from the Windows Phone Store.

**Chrome OS**

Clientless features (Portal Access, Citrix and VMware Webtop based launch) are supported on Chrome OS.

**Java Compatibility Matrix**

F5 Networks supports Java SE 6, Java SE 7, and Java SE 8. Java-related features cannot be utilized using Google Chrome on OS X and Linux because Google Chrome does not support Java plugin on OS X and Linux.

**Go to appendix A for procedure to verify the compatibility of your browser.**

Administrator Rights

The SSL/VPN device requires a browser plugin/Add-on’s to create the secure tunnel. Administrator rights on your computer are required to install this plug-in. This plug-in is automatically installed after being authorized to install during the login process. In some instances the SSL/VPN plug-in is required to be installed manually. The process to manually install the SSL/VPN is located in appendix B.

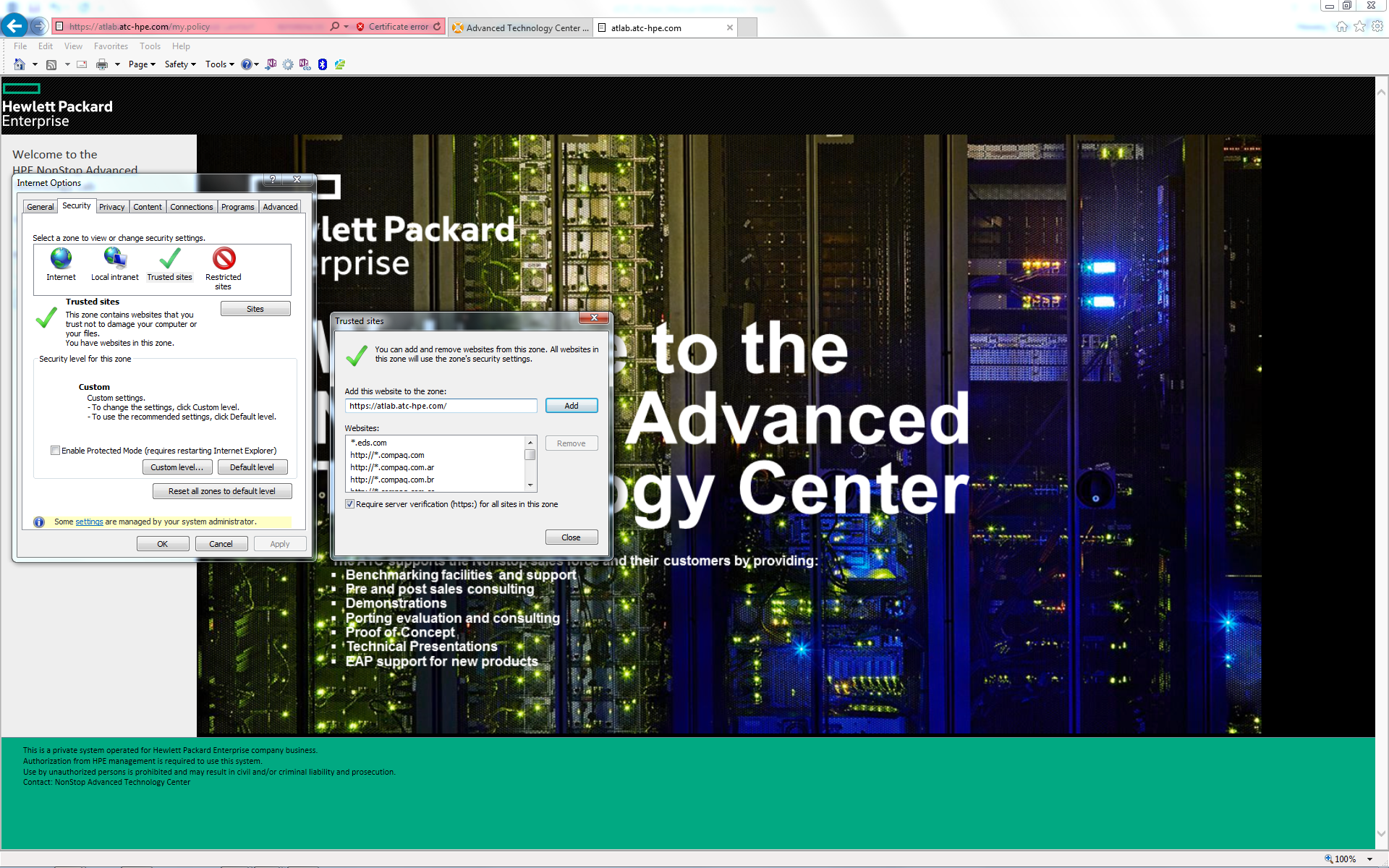
Trusted Sites

This step is not required but is inserted here as a helpful hint to overcome Firewall issues when accessing the NonStop ATC lab. This section adds the NonStop ATC URL to your Trusted Sites in IE. The NonStop ATC URL is: <https://atlab.atc-hpe.com>

Follow this process to add <https://atlab.atc-hpe.com> to your Trusted Sites in IE.

1. Open your IE browser
2. Click the “Tools” tab
3. Select “Internet Options” on the bottom of the dropdown menu
4. Click the “Security” tab
5. Select “Trusted Sites” in the “Zone to view or change” box
6. Click on the “Sites” button
7. In the “Add this website to the zone”, Enter <https://atlab.atc-hpe.com> and click the “Add” button.

Review the following screen shot for reference.

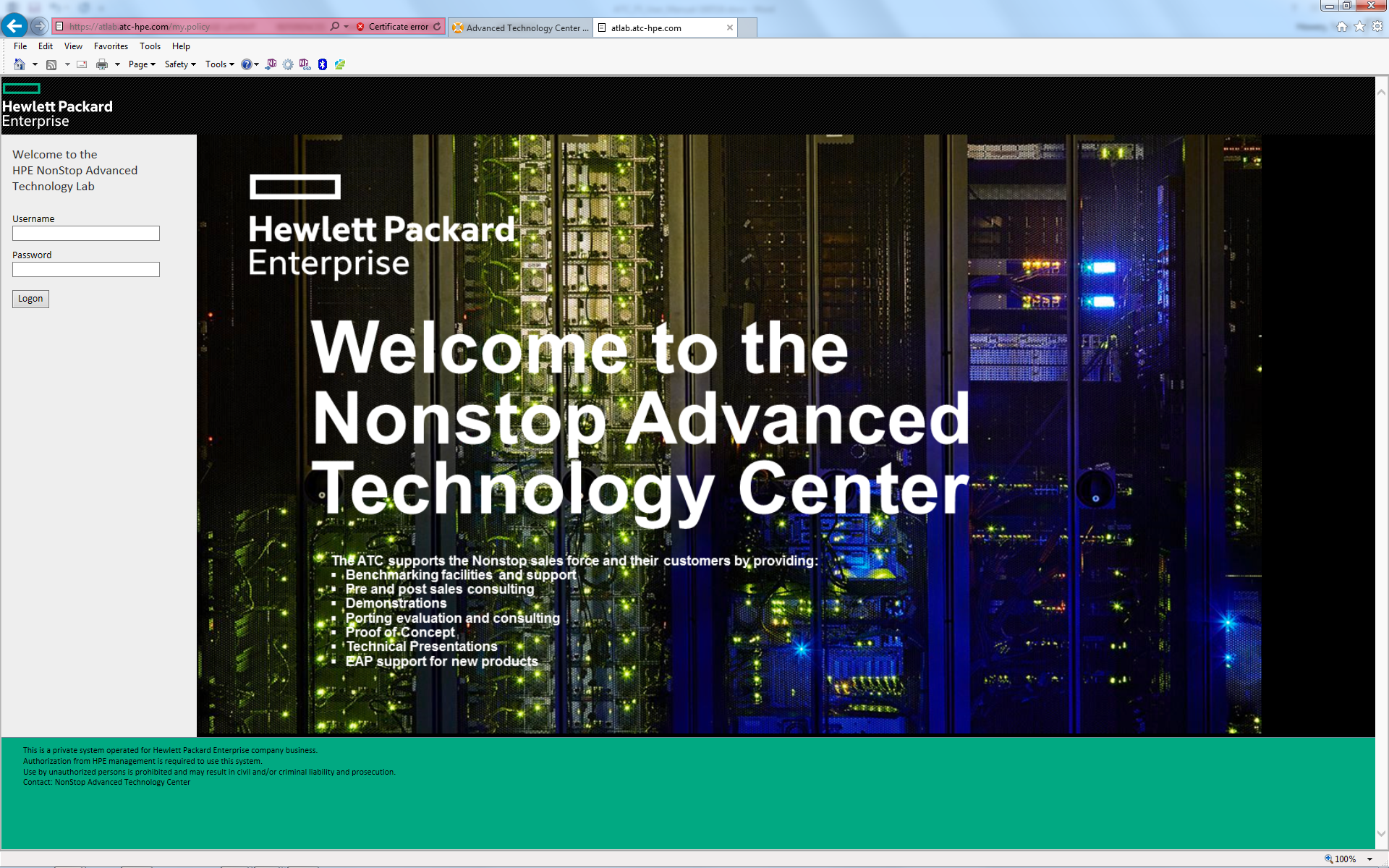


Go to the Remote Access Page

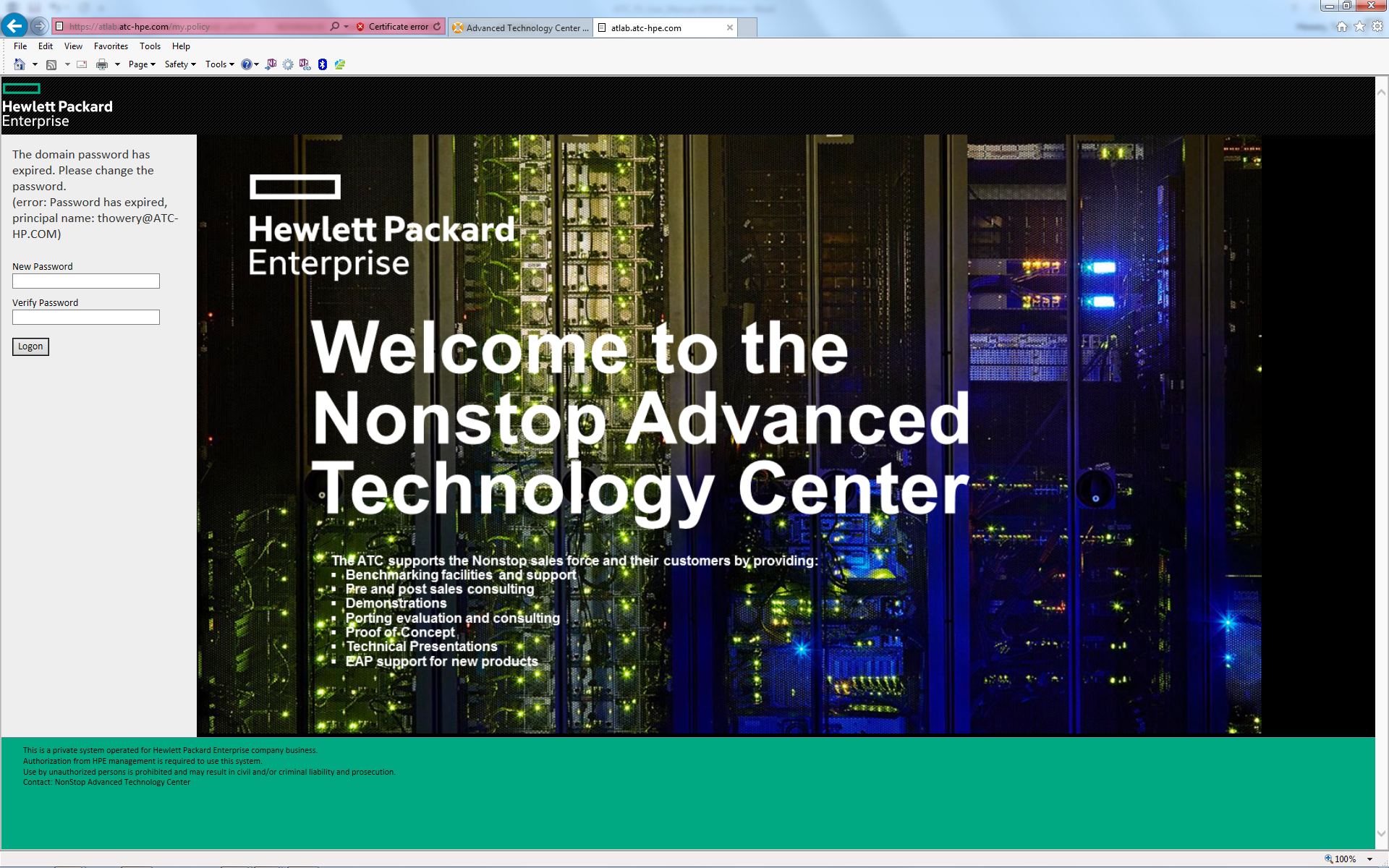
Now that your browser meets the access criteria, everything is ready to go:

<http://atlab.atc-hpe.com>

The Home page for atlab.atc-hpe.com is shown below.



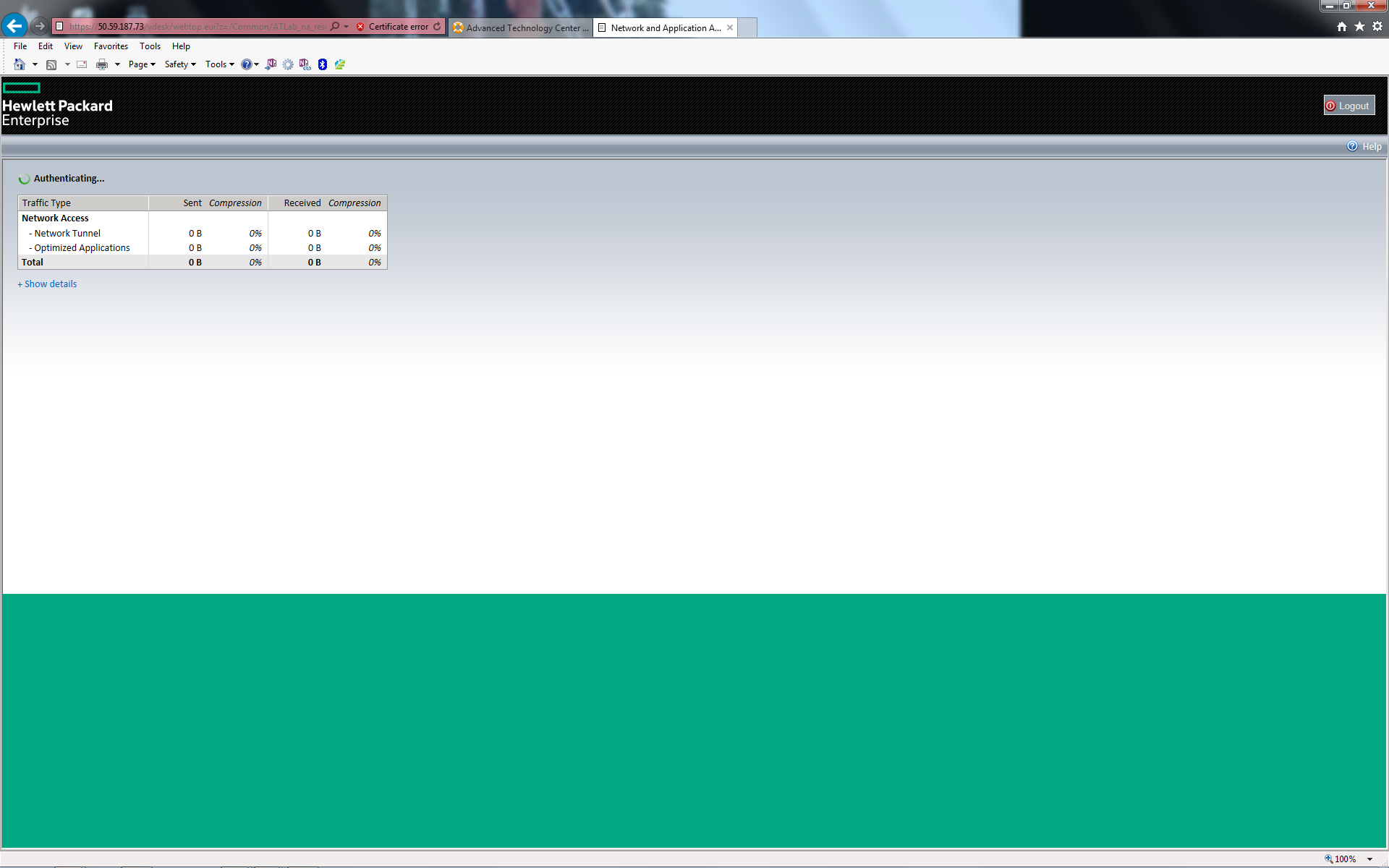
Changing your password



On your first successful login, you will be requested to change your password. Please follow the prompt and change your password.

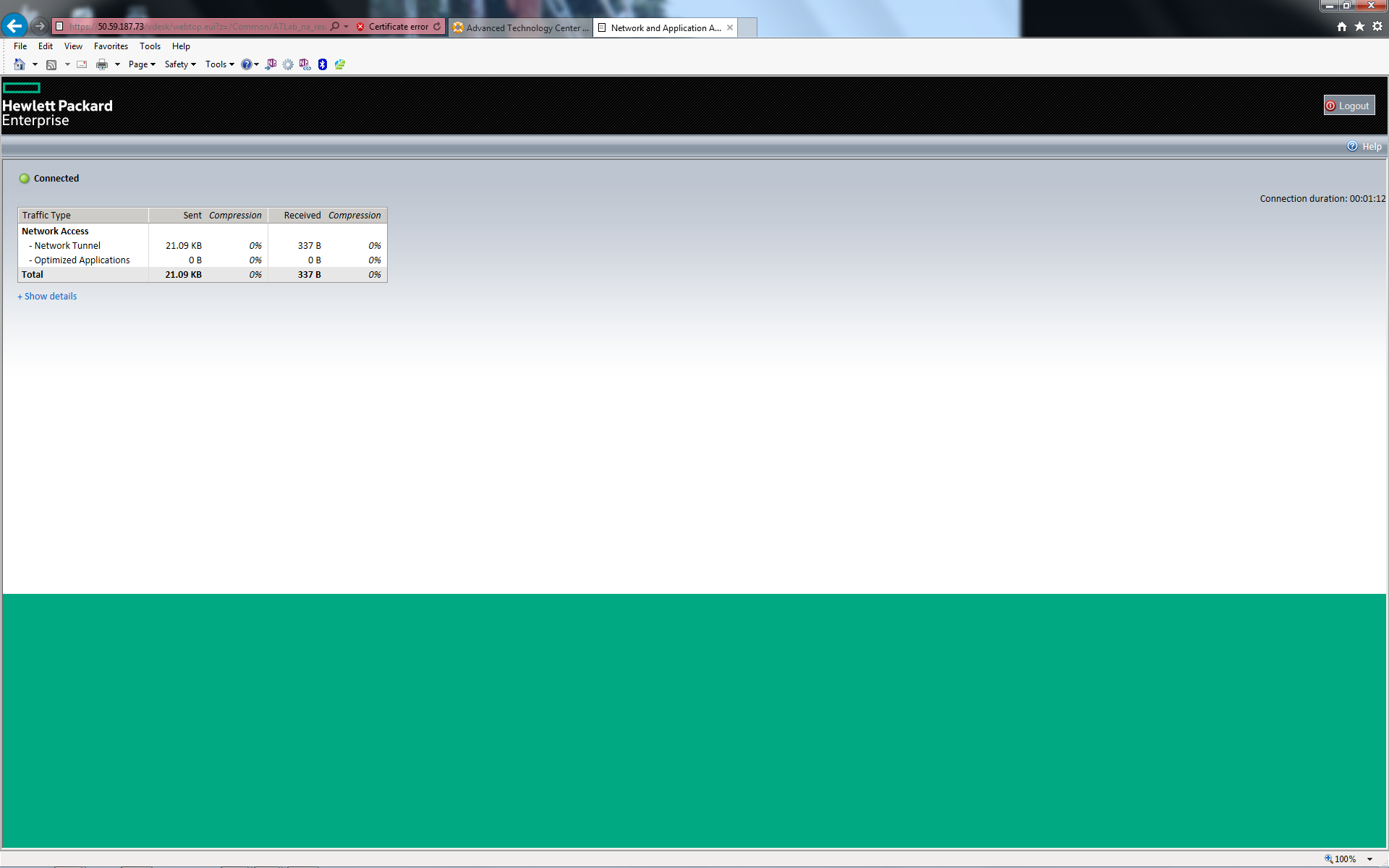
# Login Status

After you log in with your assigned username and password, you will see the following status page.



This page will display the progress of your connection. The status of your connection is shown just above the Network Access statistics box. After the status shows “Connected” you can minimize this browser window. Do not close this browser window. You will use it to terminate the SSL/VPN tunnel into the ATLab.

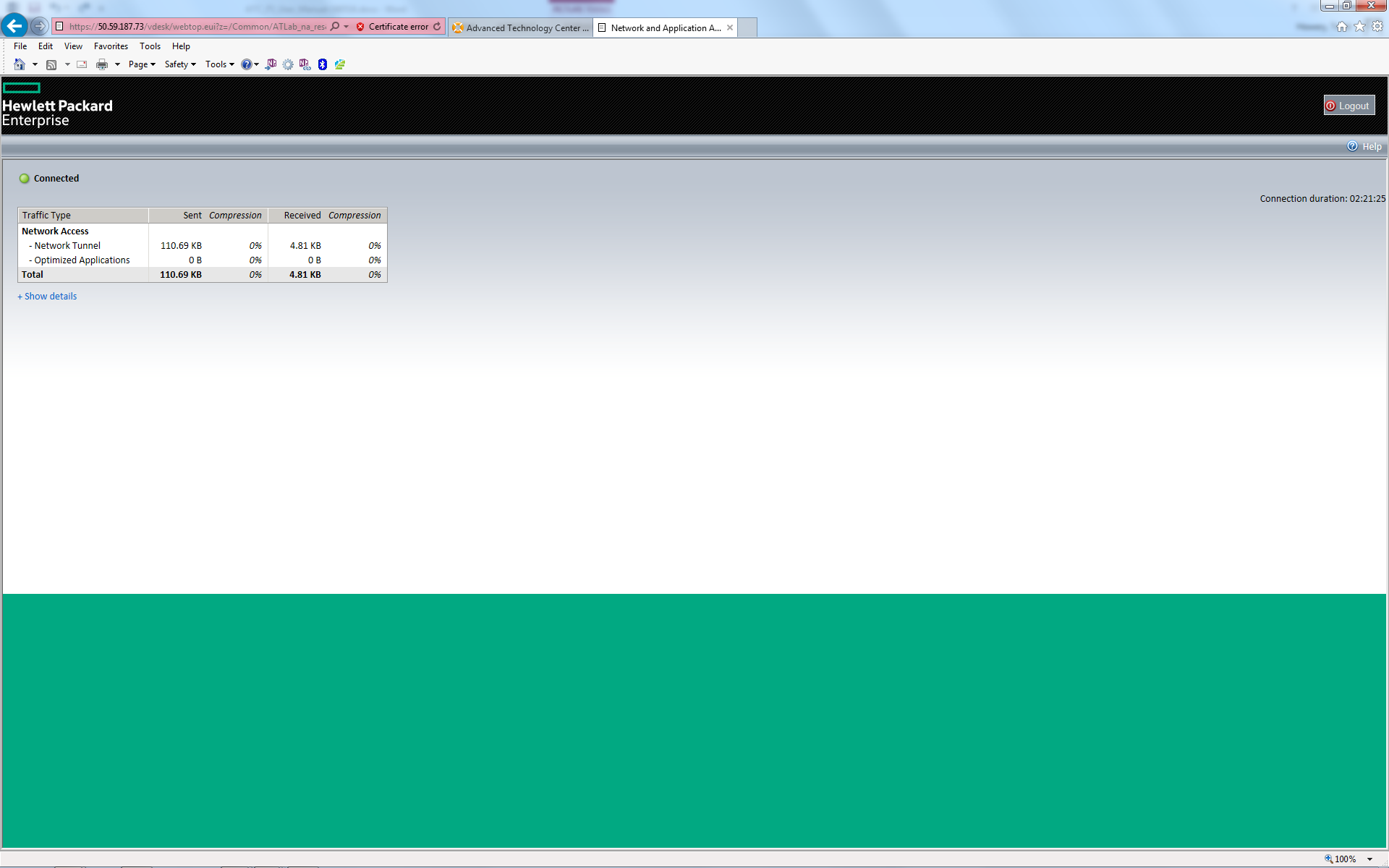
Successful SSL/VPN Tunnel



This browser graphic highlights the “Connected” status indicator on the top left corner of the display.

Terminate the SSL/VPN Tunnel

To terminate and exit the SSL/VPN tunnel into the ATLab, restore the SSL/VPN connection browser window and click on “Logout” in the upper right corner of the SSL/VPN connection page. After clicking “Logout” your SSL/VPN tunnel session will end and your SSL/VPN browser window will show your connection status as “Your session has finished”. An example of this window is shown below.



### Appendix A

How to check for 32-bit browser in IE

In 64-**bit** versions of Windows, you can determine whether you're using a 32 or 64-**bit** browser in the Task Manager:

1. Pressing **Alt** + **Ctrl** + **Delete** at the same time.
2. Clicking **Task Manager.**
3. Click the **Processes** tab.
4. The number that appears after the process for your browser indicates the version in use.
5. If the version is 64-bit, please see [Answer 7883](http://247pearsoned.custhelp.com/app/answers/detail/a_id/7883/session/L2F2LzEvdGltZS8xMzg5MDM1Mjk3L3NpZC9JY2k5KklKbA%3D%3D) for help using a 32-bit browser in a 64-bit version of Windows.

### Internet Explorer for Windows 7 and 8

Windows 7 and 8 include a 32-bit version of Internet Explorer, so no additional installation is necessary. To run it, go to **Start** > **Computer** > **Local Disk** > **Program Files (x86)** > **Internet Explorer** and double-click the file **iexplore.exe**.

If your version of Windows does not include a 32-bit version of Internet Explorer, you can install one by going to <http://windows.microsoft.com/en-US/internet-explorer/products/ie/home>.

If you're still unable to run a 32-bit version of Internet Explorer, please contact [Microsoft Support](http://support.microsoft.com/).

### Appendix B

# Manually Installing IE Browser Add-on

Please follow the links below for detailed procedures on “How-to” install IE Add-ons

<http://www.wikihow.com/Add-Addons-in-Internet-Explorer>

<http://pcunleashed.com/internet-explorer/how-to-install-add-ons-in-internet-explorer-9/>

<http://docs.moodle.org/25/en/Installing_add-ons>

http://www.mydigitallife.info/how-to-uninstall-delete-and-remove-ie-add-ons-or-extensions-permanently/

Manually Installing Firefox Browser Plugin

Please follow the links below for detailed procedures on “How-to” install Firefox Plugins

<https://support.mozilla.org/en-US/kb/find-and-install-add-ons-add-features-to-firefox>

<http://www.wikihow.com/Install-Firefox-Extensions>

<http://kb.mozillazine.org/Installing_extensions>

https://support.mozilla.org/en-US/kb/disable-or-remove-add-ons

How to Remove SSL/VPN Components

1. Download <https://firepass.fpfaq.com/sandbox/f5wininfo.exe>
2. Run the program as an administrator.
3. Tools > Remove Components > Yes
4. Close the program