1. OVERVIEW

OVERVIEW

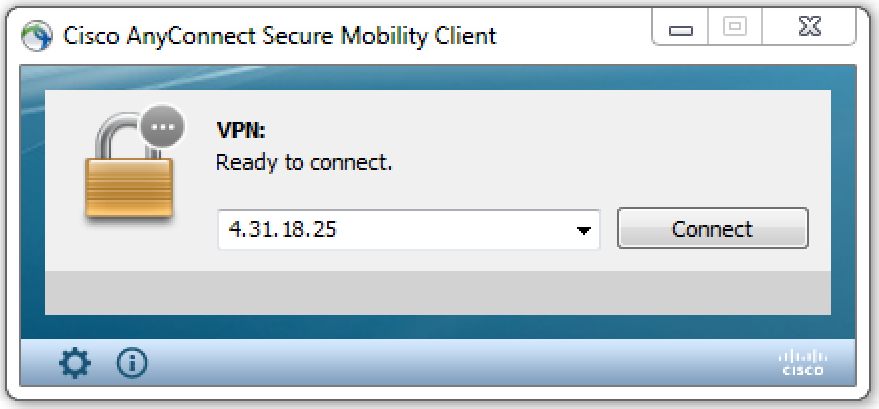
The EECS Department provides eecsNET to support Cadet and faculty with a network capable of supporting research and education requirements incompatible with the high security standards of the USMA enterprise network. It allows access to the Internet without connecting through the DREN or other DoD networks. This guide shows you how to establish a VPN connection to remotely access the eecsNET from any location. This guide also walks you through how to set-up a wifi connection to eecsNET in TH115, TH172, TH176 or TH176. ***Ensure you are VPN'ed into the eecsNET or connected to the eecsNET wifi before starting or resuming any virtual machines (VMs). This will ensure that the VMs will only communicate on acceptable networks.***

ACCEPTABLE USE

eecsNET resources may only be used by Cadets for officially sanctioned events/activities related to an academic course or department sponsored club. Use of the network for any other purpose is unauthorized unless coordinated ahead of time with an EECS faculty or staff member. Tools and techniques used on eecsNET are not meant for use on any other network and should not be used elsewhere without explicit permission of the network owner. All cadets are expected to sign and adhere to the written user agreement presented each semester at the start of classes.

Access to eecsNET is a privilege and unauthorized activities would undermine the department's ability to provide this resource in the future. Failure to adhere to applicable policies and regulations could lead to significant administrative and legal consequences such as separation or criminal charges. If you're not sure if something is OK ask your instructor ahead of time!

2. EECSNET VPN AND WIFI ACCESS


Cisco AnyConnect Secure Mobility Client

VPN:
Ready to connect.

4.31.18.25

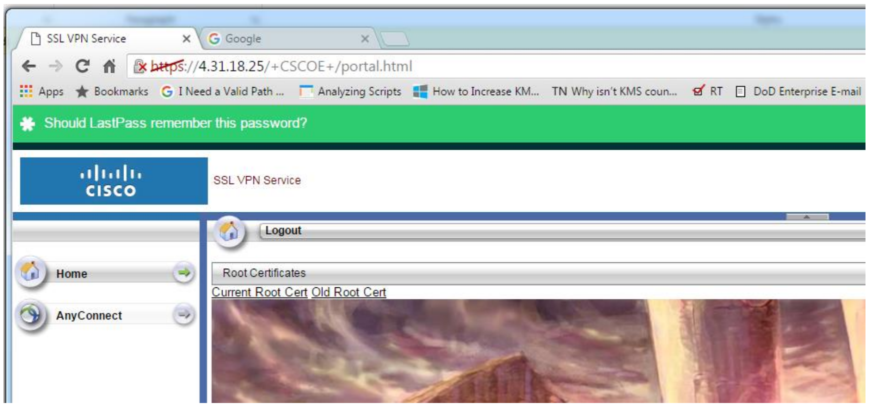
eecsNET resources can be accessed from outside of the lab environments through the VPN Gateway depicted in Section 2 or via WiFi in the various labs within the department. To access WiFi or the VPN you must have an account, which will be provided by your instructor at the beginning of the semester. ***Additionally, your computer will need to install the eecsNET CA certificate as a trusted root certificate—do this first!***

VPN SOFTWARE

The Cisco AnyConnect Secure Mobility Client is required for accessing the eecsNET VPN. It should already be installed on all USMA laptops. If you are using another device to connect you can download the appropriate software package from the VPN server Web Portal at https://4.31.18.25

EECSNET ROOT CERTIFICATE

All users must connect to the web portal to set their passwords before first login. Passwords must be at least 12 characters long. Once you complete this step and log in to the portal page you should download the two eecsNET root certificates pictured below:


~~https~~://4.31.18.25/+CSCOE+/portal.html

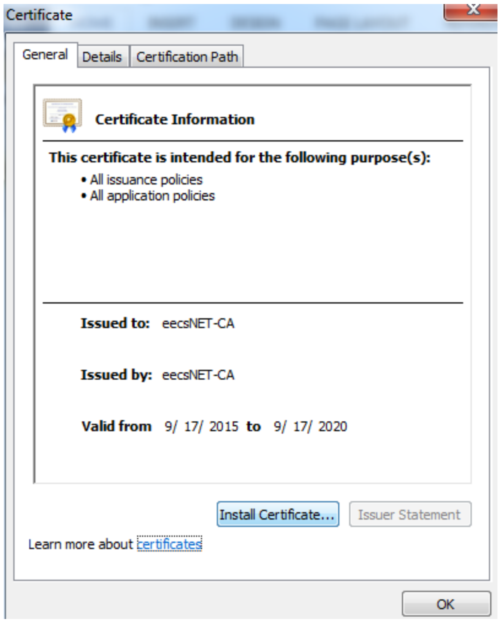
Should LastPass remember this password?

SSL VPN Service

Root Certificates

Current Root Cert Old Root Cert

Once downloaded you can right click to install the certificates via the pop-up menu. Make sure to install them to the Trusted Root Certification Authority store as depicted:



Certificate Information

This certificate is intended for the following purpose(s):

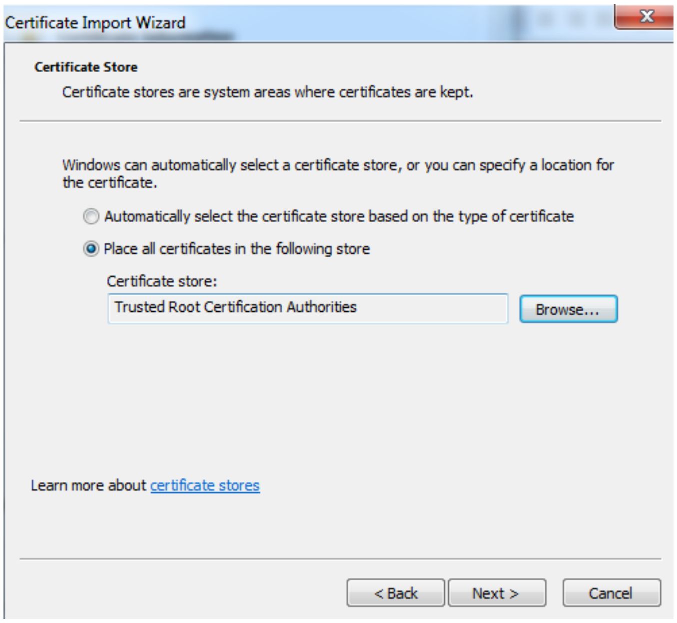
- All issuance policies
- All application policies

Issued to: eecsNET-CA

Issued by: eecsNET-CA

Valid from 9/ 17/ 2015 **to** 9/ 17/ 2020

Learn more about certificates



Certificate Store

Certificate stores are system areas where certificates are kept.

Windows can automatically select a certificate store, or you can specify a location for the certificate.

○ Automatically select the certificate store based on the type of certificate

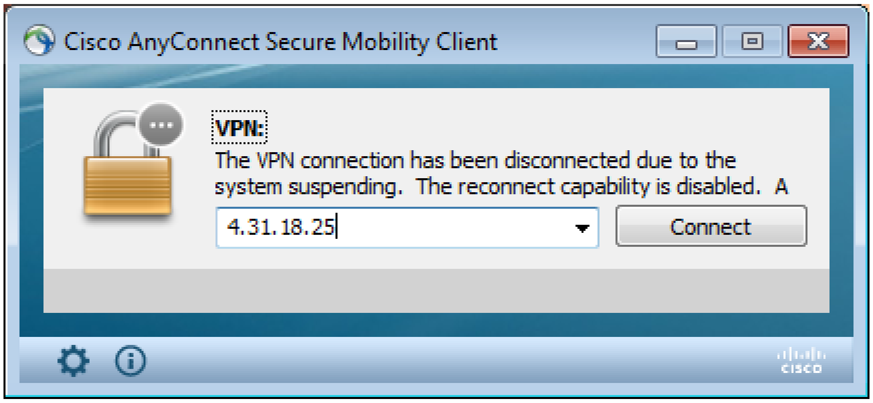
● Place all certificates in the following store

Certificate store: Trusted Root Certification Authorities

Learn more about certificate stores

ACCESSING EECSNET VIA VPN

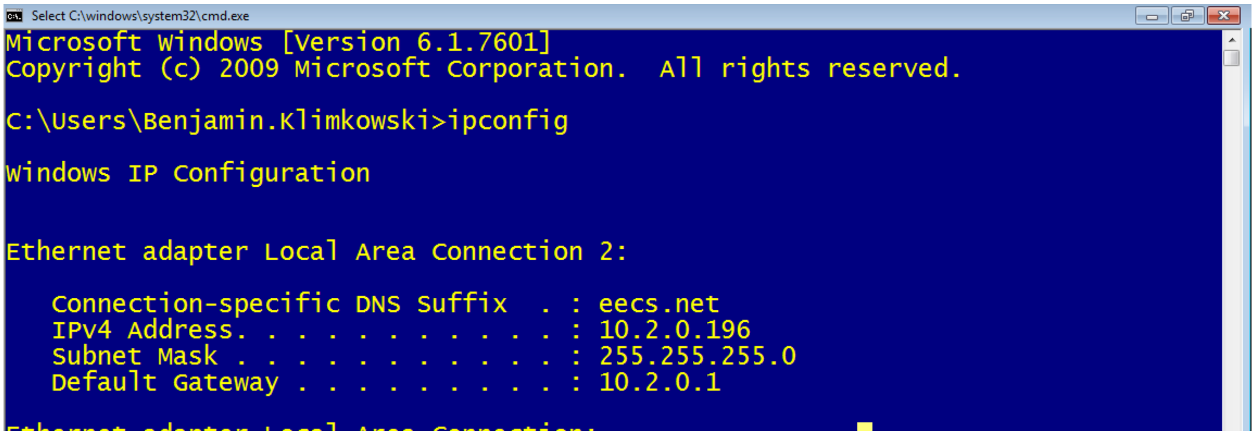
Once the certificate is installed you can access eecsNET via VPN by simply typing the IP into the Cisco AnyConnect Client and pressing connect.



VPN:
The VPN connection has been disconnected due to the system suspending. The reconnect capability is disabled. A

4.31.18.25

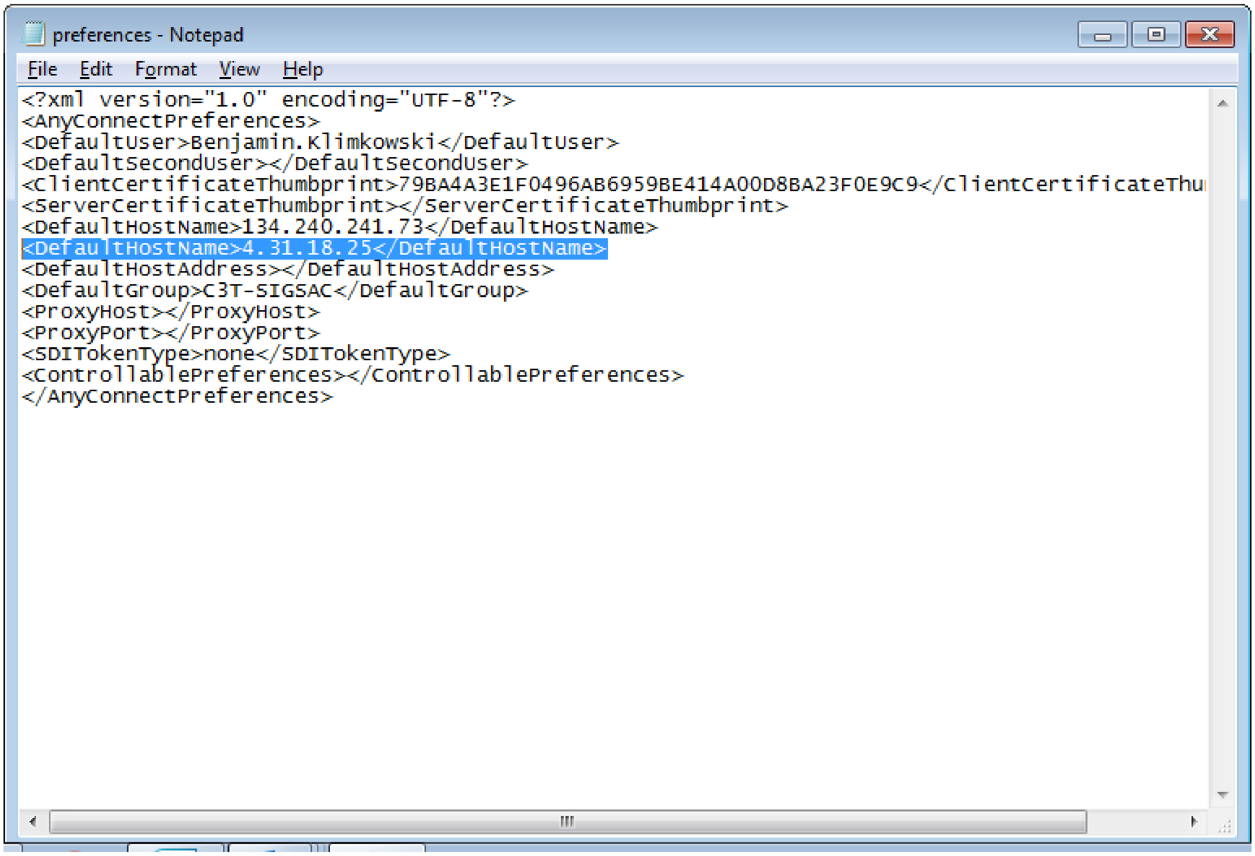
After being connected you should be see "connected," and you can verify your access by issuing "ipconfig" from the command prompt:



```
Microsoft Windows [Version 6.1.7601]
Copyright (c) 2009 Microsoft Corporation.  All rights reserved.

C:\Users\Benjamin.Klimkowski>ipconfig

Windows IP Configuration


Ethernet adapter Local Area Connection 2:

   Connection-specific DNS Suffix  . : eecs.net
   IPv4 Address. . . . . . . . . . . : 10.2.0.196
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . : 10.2.0.1

Ethernet adapter Local Area Connection:
```

ADDING A PERMANENT PROFILE

Right click on the toolbar and quit the VPN client. You can make 4.31.18.25 a permanent part of your VPN profile by adding a line to the preferences file located at C:\Users\YOURUSERNAME\AppData\Local\Cisco\Cisco AnyConnect Secure Mobility Client:



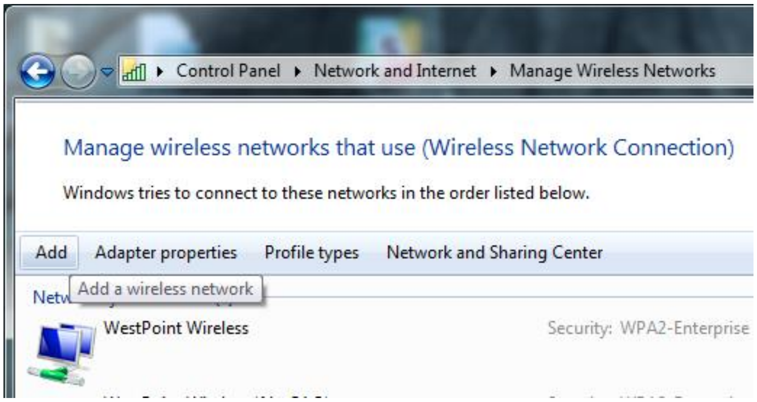
```
<?xml version="1.0" encoding="UTF-8"?>
<AnyConnectPreferences>
<DefaultUser>Benjamin.Klimkowski</DefaultUser>
<DefaultSecondUser></DefaultSecondUser>
<ClientCertificateThumbprint>79BA4A3E1F0496AB6959BE414A00D8BA23F0E9C9</ClientCertificateThu
<ServerCertificateThumbprint></ServerCertificateThumbprint>
<DefaultHostName>134.240.241.73</DefaultHostName>
<DefaultHostName>4.31.18.25</DefaultHostName>
<DefaultHostAddress></DefaultHostAddress>
<DefaultGroup>C3T-SIGSAC</DefaultGroup>
<ProxyHost></ProxyHost>
<ProxyPort></ProxyPort>
<SDITokenType>none</SDITokenType>
<ControllablePreferences></ControllablePreferences>
</AnyConnectPreferences>
```

Restart the client and you should see the IP listed in the drop down.

WIFI CONFIGURATION

eecsNET Access Points utilize WPA2 Enterprise to provide user authentication. If you are using a USMA laptop make sure to follow these steps or you will not be able to connect.

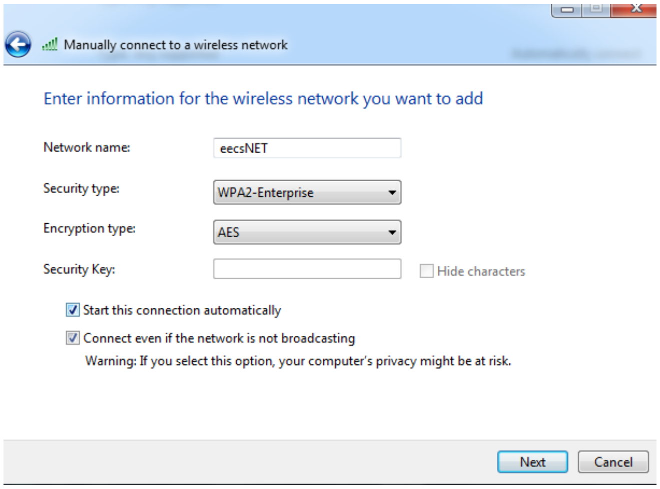
Manually create a wireless network for the appropriate SSID in your lab


Control Panel ▸ Network and Internet ▸ Manage Wireless Networks
Add
Adapter properties
Profile types
Network and Sharing Center
Add a wireless network
Netw

Manage wireless networks that use (Wireless Network Connection)

Windows tries to connect to these networks in the order listed below.

WestPoint Wireless   Security: WPA2-Enterprise



Manually connect to a wireless network

Enter information for the wireless network you want to add

Network name:	eecsNET
Security type:	WPA2-Enterprise
Encryption type:	AES
Security Key:	□ Hide characters

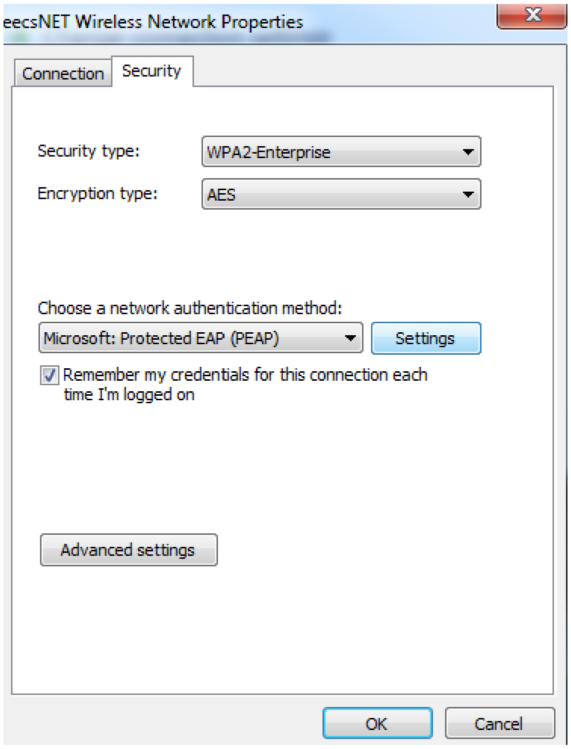
☑ Start this connection automatically

☑ Connect even if the network is not broadcasting

Warning: If you select this option, your computer's privacy might be at risk.

The authentication protocol should be set to PEAP

In the advanced configuration settings make sure that eecsNET CA is checked as trusted



eecsNET Wireless Network Properties

Connection | Security

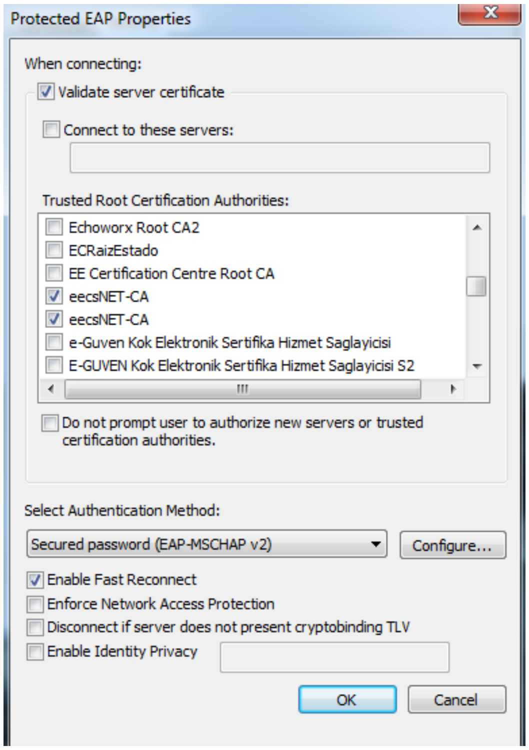
Security type: WPA2-Enterprise

Encryption type: AES

Choose a network authentication method:

Microsoft: Protected EAP (PEAP) | Settings

☑ Remember my credentials for this connection each time I'm logged on



Protected EAP Properties

When connecting:

☑ Validate server certificate

☐ Connect to these servers:

Trusted Root Certification Authorities:

- ☐ Echoworx Root CA2
- ☐ ECRaizEstado
- ☐ EE Certification Centre Root CA
- ☑ eecsNET-CA
- ☑ eecsNET-CA
- ☐ e-Guven Kok Elektronik Sertifika Hizmet Saglayicisi
- ☐ E-GUVEN Kok Elektronik Sertifika Hizmet Saglayicisi S2

☐ Do not prompt user to authorize new servers or trusted certification authorities.

Select Authentication Method:

Secured password (EAP-MSCHAP v2) | Configure...

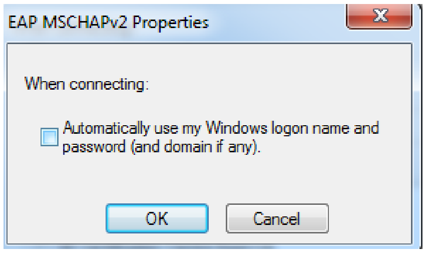
☑ Enable Fast Reconnect

☐ Enforce Network Access Protection

☐ Disconnect if server does not present cryptobinding TLV

☐ Enable Identity Privacy

Click the Configure box and ensure that your logon credentials are not automatically being passed.



EAP MSCHAPv2 Properties

When connecting:

☐ Automatically use my Windows logon name and password (and domain if any).