Gateway Community College

Technical Support
TABLE OF CONTENTS

SECTION
CLASSROOM SUPPORT AND HELP DESK ................................................................. 3
SECTION II
INFORMATION TECHNOLOGY SERVICE LEVEL AGREEMENT .................................... 4-7
SECTION III
COMPUTER LOG IN PROCEDURE FOR NEW USERS .................................................. 8
SECTION IV
NET ID AND STUDENT PASSWORD CHANGES ....................................................... 9-10
SECTION V
THE MYCOMMNET PORTAL AND FACULTY LOG IN ................................................ 11-12
SECTION VI
GUIDE TO MYCOMMNET FOR STUDENTS, FACULTY & STAFF ............................... 13-19
SECTION VII-A
OUTLOOK WEB ACCESS LOG IN (E-MAIL FOR FACULTY & STAFF) ......................... 20-21
SECTION VII-B
HOW TO ADD YOUR OUTLOOK EMAIL TO YOUR CELLPHONE OR IPAD (FACULTY & STAFF ONLY) ................................................................. 22
SECTION VIII-A
HOW TO ACCESS YOUR OFFICE365 EMAIL ACCOUNT (STUDENTS ONLY) ................ 23
SECTION VIII-B
HOW TO ADD OFFICE365 EMAIL TO YOUR CELLPHONE OR IPAD (STUDENTS ONLY) ......................................................................................... 24
SECTION IX
HOW TO DOWNLOAD MICROSOFT OFFICE 365 (STUDENT, FACULTY & STAFF) ........ 25-27
SECTION X
HOW TO SETUP YOUR ONEDRIVE FOR BUSINESS ................................................ 28-29
SECTION XI
HOW TO ACCESS CLASS ROSTER (FACULTY ONLY) ................................................ 30-32
SECTION XII
HOW TO INPUT MIDTERM AND FINAL GRADES (FACULTY ONLY) ......................... 33-36
SECTION XIII-A
PROTECTIVE ENCLAVE AND MULTI-FACTOR AUTHENTICATION (MFA) ............... 37-50
SECTION XIII-B
HOW TO CHANGE YOUR MULTI-FACTOR AUTHENTICATION (MFA) SETTINGS ........ 51-56
SECTION XIII-C
HOW TO ACTIVATE THE MOBILE APP ....................................................................... 57-61
SECTION XIV-A
CAMPUS WIRELESS ACCESS .................................................................................. 62-63
SECTION XIV-B
MAC OS WI-FI ACCESS INSTRUCTIONS ................................................................. 64
SECTION XIV-C
HOW TO CONNECT TO THE WI-FI USING YOUR IPHONE & IPAD ....................... 65-67
(STUDENTS, FACULTY & STAFF)
SECTION XIV-D
HOW TO ACCESS THE WIFI USING YOUR IPHONE, IPAD, & ANDROID ................... 68
(FACULTY & STAFF ONLY)
I- Classroom Support and Help Desk

There are several ways to obtain classroom support. You may call our Help Desks by phone, you may use our email drop box, you may visit us in person, or you may use the repair slips that are posted in the computer classrooms. (an example of our repair form is posted below.)

Our Help Desks is located in Room N323 and our contact number is 203-285-2040.

Our regular office hours are: Monday-Thursday: 7:00am to 9:00pm, Friday from 8:00am to 6:00pm, and from 7:30am to 1:00pm on Saturdays.

We cover all technical aspects of the classroom, including computer hardware and software issues, printing and networking issues, and password and log in issues.

The Help Desk also provides support for all administrative computing functions, including e-mail, Banner, all college-owned and operated desktop software and hardware, and networking and connectivity issues.

Please note that Help Desk support is limited to Gateway Community College faculty, staff and students.

Contacts:
Email- gw-HelpDesk@gwcc.commnet.edu (This email is automatically forwarded to all IT department personnel.)
Phone- 203-285-2040
In Person- During office hours- Room N323
II- Information Technology Service Level Agreement

Key Metrics
- Tier 1 service request (phone, email, walk-in) answered by a live person: 70%
- Tier 1 service request (phone, email, walk-in) resolution on the first call: 60%

Overview
This Service Level Agreement (SLA) defines the services and service levels between the service provider, the Information Technology Department (IT Dept.), and the customers of that service (Customer). Eligible customers are the faculty, staff, students and visitors to Gateway Community College.

Service Description
The IT Dept. provides an efficient, cost-contained approach for the college IT support functions. The IT Dept. starts with friendly, knowledgeable staff who understand your technical environment. This team of experts is supported by a technical infrastructure that allows us to deploy applications, updates and patches, as well as detect problems.

Intended Users
Faculty, staff, students and visitors of the college.

Supported Computing Environment
Managed IT Support provides desktop support for college-owned equipment for faculty and staff, and provides connectivity services and basic support for students and visitors in all campus locations.

Technical Support
Both Tier 1 and Tier 2 technical support are available from 7 a.m. to 5 p.m. Monday through Friday, excluding all holidays and college closures. Tier 1 support is also available from 5 pm to 9 pm, Monday through Thursday evenings, and from 8 am to 12 30 pm on Saturdays.

Tier 1
There are three ways customers can contact the IT Dept. for support:
- Phone (203) 285-2040
- Via email to gw-helpdesk@gwcc.commnet.edu
- Walk in service to our office in room N323.
Initial Response

1. Requests for support will be fulfilled based on priorities (Critical, High, Medium, Normal) which are determined by urgency and level of impact; and the order in which the call was received.

2. Response is defined as a “good faith” effort to communicate with the customer using the contact information provided by that customer. Response may be via phone or voice mail, email, or personal visit.

3. Service Level response times to service requests are measured once a request is submitted. All service requests are to be made directly to the Help Desk via phone, email or walk-in.

Emails and phones calls to individual support personnel will delay the response to your request.

Status Definitions with Initial Response Times

- **Critical** - Within 30 minutes: Catastrophic inability to complete job duties. Example: computer does not turn on or boot up properly; Instructor computer in classroom not working.

- **High** - Within 2 business hours: Loss of a major job duty. Example: E-mail not working, not connected to internet, inability to print at all. VoIP (basic) not working, no phone service. Example: cannot receive incoming calls and cannot make outgoing calls.

- **Medium** - Within 1 day: There is a problem to be solved, but customer is still functional and has other options available. Example: Desktop printer is not working, but customer has access to departmental printers. VoIP (basic) phone working but voice mail not working.

- **Normal** - Within 2 days: General request for software or computer installations or other tasks that are not time sensitive. Example: User needs help but will not be available until a few days later. General requests for VoIP (basic), such as, feature changes, phone relocation, adding/changing service, and new phone.

If your service request is not responded to in these defined time frames, please call the Help Desk at ext. 52040 to check on the status of your call, as it may be delayed due to volume.

Tier 2

Issues that cannot be resolved by tier 1 support personnel or methods will be escalated to the IT Dept. support person who can resolve the issue.

Other Services
Patch Management

By default, desktops and laptops installed by the IT Dept. are enrolled into automated software updates. For PCs, updates are deployed via Altiris and WSUS and for Macs, via Altiris. Customers are notified via e-mail in advance of each monthly update deployment. Microsoft out-of-band and third-party critical updates (such as Java, Flash Player, and Adobe Reader) are deployed as they become available.

Responsibilities

Customer responsibilities in support of this agreement include:

• Request help and services defined in Technical Support of this SLA.
• When requesting help, contact the Help Desk directly to receive the quickest response. Please see Technical support, Tier 1, Initial Response for the ways to contact the Help Desk.
• Respond to IT Dept. staff inquiries in a professional and timely manner.
• Provide the IT Dept. with timely physical access to supported systems.
• Maintain compliance with all software licensing requirements.
• Adhere to relevant College acceptable use, security policies and standards.
• Only IT personnel are authorized to diagnose, reconfigure or remove IT equipment.
• Use IT as a strategic partner when looking to purchase new hardware or software, or when looking to purchase or develop new technology-based systems.
• Categorize data according to the college data management policy and state retention standards where applicable. The user or customer is the owner of their data.
• Data Managers review and approve departmental personnel administrative access to supported systems, based on business requirements.
• Any position that gives users access to Banner or DCL 3 data- employees are required to complete the appropriate training before the access is granted.

IT Dept. responsibilities in support of this agreement include:

• Ensure workstations and devices meet standards established by college and BOR policies, including acceptable use and security mandates.
• Effectively and efficiently deploy operating systems, applications, software patches and updates.
• Respond to customer inquiries in a professional and timely manner. Response times are defined above in Technical Support, Tier 1, Status Definitions and Response Times.
• Establish real time monitoring of device performance, compliance and inventory.
• Minimize disruptions of customer production when desktop maintenance and support operations are performed.
• Provide recommendations on hardware life cycle.
• Maintain a hardware and software inventory.
• Coordinate maintenance, repair, and/or replacement for in-warranty hardware.
• Coordinate and troubleshoot network connectivity, including wireless connectivity.
• Advise customers on security, networking or information technology best practices, policies, or requirements.

Definitions

**Altiris**- The software system that allows IT to image and patch campus computers in an automated fashion.

**Banner**- The college’s enterprise data system. It contains all student records, employee directory information and other college information such as room schedules and facility attributes.

**Data Manager**- A college employee, typically the Director of a department, who has responsibility to ensure that DCL 3 data is stored properly and is access only by employees who have the proper authorization and training.

**DCL3 Data**- Confidential data that if breached, could result in financial loss to the college. Examples include Social Security numbers, bank account numbers, credit card numbers, driver’s license numbers and financial aid data. This data should only be accessible to authorized, trained personnel.

**VoIP**- Voice over IP, or a telephone system running over the campus network, as opposed to dedicated phone lines.

**WSUS**- Windows Server Update Service, a Microsoft technology that allows us to choose and deploy Microsoft patches on an as-needed basis.
III- Computer Log In Procedure for New Users

Press and hold down in sequence the Alt, Ctrl and the Del keys.

You will now see a box with three lines, the user name, password and the log on to.

The user name is your Banner number without the @ symbol, and with the college domain typed with it-for example, 12345678@gwcc.commnet.edu

Your initial password is the first three letters of your birth month, with the first letter capitalized, the & symbol, and the last four digits of your Social Security number.

If you are “homed” at another college, please use that college’s abbreviation in the domain part of the user name.

Once you log in for the first time, you will be prompted to change your password.

Password Requirements:

The following requirements must be followed when selecting a NetID password.

- Password must be at least eight characters.
- Password must be complex and difficult to guess. A password must contain characters from three of the four categories:
  1. Uppercase characters (A through Z)
  2. Lowercase characters (a through z)
  3. Numeric digits (0 through 9)
  4. Special characters (for example, !, $, #, %)
- Password must not contain all or part of the user’s NetID account name.
- Password must differ from previous passwords.
- Password is forced to change every 180 days, but users have the ability to change them sooner.

Please note- if you taught last semester, or teach at another CCC college, please use the same password you have used previously. If your password has expired, the system will prompt you for a password change.

If you experience problems with your Net ID, please go to the website

http://www.commnet.edu/netid

Note: Without the security question, you cannot use the password reset website at http://supportcenter.ct.edu/netid/pswdmenu.asp

If you still have problems, please contact us.

Email- gw-HelpDesk@gwcc.commnet.edu (This email is automatically forwarded to all IT department personnel.)
Phone- 203-285-2040
In Person- During office hours- Room N323
IV- Student NetID Logon and Student Password Changes

Please note that all on campus computer users are required to logon to computers using their individual NetID and password. **COMPUTERS WILL NOT BE AVAILABLE WITHOUT YOUR NetID!**

Log On Procedure

When you log onto the computer, please make sure of the following:
The user name has to be your Banner number @student.commnet.edu
The password has to be your password.

**Protect your User Account! When you are finished using a computer, you must shut down the computer so that others do not have access to your account.**

**NetID:** The NetID is composed of the following two items
1. Your Banner number, which is your Banner ID without the @ sign.
2. Domain = @STUDENT.COMMNET.EDU

Example: Peter Guota with a BannerID of @00023546 will have the following NetID: 00023456@STUDENT.COMMNET.EDU

**NetID Password:**

Your **initial** NetID password will be a combination of personal information as follows

1. 1st three characters of birth month with first letter CAPITALIZED
2. Ampersand character (&)
3. Last 4 digits of your social Security Number

So, for a user with a birth date of 10/24/79 and SSN of 123-45-6789, then initial password would be: Oct&6789

**You will be required to change your password the first time you logon.**

**Password Requirements:**

The following requirements must be followed when selecting a NetID password.

- Password must be at least eight characters.
- Password must be complex and difficult to guess. A password must contain characters from three of the four categories:
  5. Uppercase characters (A through Z)
  6. Lowercase characters (a through z)
  7. Numeric digits (0 through 9)
  8. Special characters (for example, !, $, #, %)
- Password must not contain all or part of the user's NetID account name.
- Password must differ from previous passwords.
- Password is forced to change every 180 days, but users have the ability to change them sooner.

The following are a few suggestions for creating a secure NetID password:
Randomly pick alternating uppercase and lowercase vowels and consonants. Add in a digit or two; (e.g., eBiC92oD)

Combine three and four character words with at least one digit between them. This will create passwords that can be easily remembered but difficult to crack (e.g., Egg123Salad).

Randomly pick a book, poem, or song. Select a phrase from the work and use the first character of each word in the phrase as your password. Add in at least one digit or change some of the existing letters to digits or special characters. For example, the phrase "Four score and seven years ago our forefathers..." might become this password: 4s&7yaof

If the password you select does not meet the requirements specified above, you will get the following error message and be asked to try again:

Your password must be at least 8 characters; cannot repeat any of your previous 24 passwords; must contain capitals, numerals or punctuation; and cannot contain your account or full name. Please type a different password. Type a password which meets these requirements in both text boxes.

If you have any questions, please stop by the Information Technology Help Desk and ask for assistance.

Forgotten Passwords

A web utility has been created to allow users to reset lost or forgotten NetID Passwords. Go to one of the kiosks in the college lobbies or to the Computer Center to access this utility.

The address is www.commnet.edu/netid

Prior to resetting a password, a user will have to verify their identity by entering the following personal information in addition to their BANNER ID.

- Birth Date
- Social Security Number
- Security question (set in Self Service Banner)

Don’t Know Your Banner ID?

If you do not know your BANNER ID, see the Records Office. Be prepared to verify your identification with a picture ID. This can only be done in person.

Need Help with your Net ID or Password?

If you need assistance using your NetID, first, go to the website www.commnet.edu/netid. If you still need assistance, please call the Help Desk at ext. 52040.

When you are finished using a computer, please shut down the computer. Failure to do so can result in others using your account unethically and improperly.
V- The MyCommNet Portal and Faculty Log In

MyCommNet portal is where you access - Self-Service Banner, Blackboard Learn and the Library Databases - under single sign-on access through your NetID.

For rosters and grading purposes, it is important for you to know that you will have to go to myCommNet and use your NetID to log in and submit grades. The URL for the portal is http://my.commnet.edu. If you do not know how to use your NetID, you will not be able to submit grades and access rosters. Please come to the Information Technology Department and we will assist you in utilizing this important resource.

Your NetID is the log in that you use to access campus computers and college email, and looks like this:

User name: 87654321@gwcc.commnet.edu (your Banner number @gwcc.commnet.edu)

Password: Jan&5678 (Your 8-character or longer complex password)

If you have not logged into a campus computer or the MyCommNet portal, you will have to use your original default password, which consists of:

- The first three letters of the month you were born, with the first letter capitalized.
- The Ampersand character &
- The last four digits of your Social Security number.

For example: Sep&9876

If you have already logged into a campus computer or the MyCommNet portal, just use the same password that you have previously used.

When you are ready to log in, please go to the website http://my.commnet.edu

This is what this page looks like. Click Login and it will redirect you to CSCU Login Portal
For first-time users only—On your first log in, the system will require you to change your password. That screen looks like this:

In the Old Password box, key in your old (or default) password. In the New Password box, key in your new password. Your new password must meet the complexity requirements as indicated on the screen. In the Confirm New Password box, please type your new password in a second time.

Once you have successfully entered your new password, the system will bring you to the main portal of Mycommnet.

A reminder, you utilize the same user name and password for campus computers, MyCommNet and e-mail. This password change covers all three of these functions.

If you do not know how to use your NetID, you will not be able to submit grades and access rosters. Please come to the Information Technology Department and we will assist you in utilizing this important resource.

For assistance, please come to room N323, telephone, 203-285-2040
VI- Guide to MyCommnet for Students, Faculty & Staff

Go to: http://my.commnet.edu/

Search for Courses

The page should look like this

1. Select term (i.e. Fall Term 2019)
2. Select College
3. Select Open/Close Classes & Select Course Level
4. Select a Subject
5. Once you have made all your selections click on: Get Courses
In this page, you will see all the details of the classes you are searching.

To get access to your Grades, Schedule, Transcripts or Student Records login into MyCommNet

1. Type in your Net ID (i.e 01234567@student.commnet.edu)
2. Type in your Password
3. Login
Homepage of MyCommNet

To access, Financial Aid, Students Record, Registration & Payments
Click on: Banner Self Service
Under each tab you will find all the information you need.

For instance, Under Student Records Tab you will see:

- Transcripts
- Grade/Registration History
- Enrollment Verification Request
- Advisor and Major

Under Registration/Schedule Tab you will be able to:

- Item that may prevent registration
- Student Degree Evaluations
- Class Registration
- Student Schedule
- Term Selection
- Evaluate your course
Under Billing/Payment Tab you will find the following:

- My Account/Payment Information
- Account Summary by Term
- Tax Year Selection
- Direct Deposit Enrollment

Under Financial Aid Tab you will find the following:

- My Financial Aid Status
- Eligibility Requirements
- Award Package
- My Eligibility
- Award Payment Schedule
- Title IV Authorization
- Award History
- Loan Status
- Work-Study Employment
- Federal Chopping Sheet

Under Personal Information Tab you will find:

- Address and Phone Information
- E-mail Address Information
- Name Change Information
- Social Security Number Change Information
- Student College Contract Information
- MyCommNet Alert Information
Under Selective Programs Tab you will find:

- Nursing Application
- Nursing Required Items
- Nursing Decisions
- Allied Health Application

If you have any more questions regarding MyCommNet please contact the IT Helpdesk at 203-285-2040 or email us at GW-Helpdesk@gwcc.commnet.edu

If you want to Access Blackboard Learn

Click on: Blackboard Learn
Once you click on Blackboard Learn, it will open a new window that looks like this.

In here you will see all your online classes that you have register for it. If you have any more questions regarding Blackboard Learn please contact Lynn Roller at 203-285-2295.

If you have any questions, feedback or comments please contact.
Lawrence Salay
Director of Information Technology
203-285-2046
lsalay@gwcc.commnet.edu
A. Outlook Web Access Log In (E-Mail for Faculty & Staff)

All faculty and Staff, including all adjunct faculty are issued e-mail accounts.

Accessing your email from off-campus or through the Internet is a critical function that most faculty and adjuncts have to perform on a regular basis.

First you need to know your log in, or as it is also called, your NetID. Your NetID is your Banner Number with the college domain, and your 8 characters or longer complex password. Your NetID is described in detail in Section I, and is the same as what you use to get into MyCommNet.

Your email address is different than your NetID. Your email address is your first initial and last name, combined with the college domain. For example, if your name is Steve Smith, then your email address would be ssmith@gwcc.commnet.edu

To access your email, go to the website https://login.microsoftonline.com

The page will look like this: Type your full NetId and it will redirect you to the CSCU Login Portal.

** Sign in with your NetID and Password.
Once you are in, the screen will look like this.

You can then communicate with your colleagues and students easily and directly.

Email is also accessible from MyCommNet.
VII- B. How to add your Outlook email to your Cellphone or Ipad (Faculty & Staff Only)

IPad/IPhone Settings:

Note: Before adding your email, you must set a passcode for your cellphone.

• Settings
• Click on: Mail, Contacts
• Click on: Add an Account
• Select: Microsoft Exchange
• Enter your email: (outlook email address) e.g., EMAILADDRESS@gwcc.commnet.edu
• Enter password (Mycommnet password)
• In the Server Field type in: outlook.office365.com
• Domain: (leave this blank)
• Username: (full NetID) e.g 01234567@gwcc.commnet.edu
• Password: MyCommnet password
• Description: Leave this blank
• Click on: Next
• Click on: Save

Your Gateway email account is now set up on your mobile device.

Android Settings:

Note: Before adding your email, you must set a passcode for your cellphone.

• Settings
• Click on: Add account
• Select: Corporate or MS Exchange
• Enter your email: (outlook email address) e.g., EMAILADDRESS@gwcc.commnet.edu
• Enter Password: MyCommnet password
• Click on: Next
• Type your NetID in the field designated “User Name” (e.g., 01234567@gwcc.commnet.edu)
• In the Server Field type in: outlook.office365.com
• Select: Secure SLL
• Click on: Activate

Your Gateway email account is now set up on your mobile device.

Please note: you must use gwcc.commnet.edu, gatewayct.edu will not work.

This is a general guide to add an email account onto Android cellphones- your settings may be slightly different.
VIII- A. How to access your Office 365 email account (Students Only)

1. Login into: http://my.commnet.edu

2. Click Login then Type in your NetID (01324567@student.commnet.edu). Then, type in your password. If this is your first time, login with your default password which will be the first three letters of your birth month, the ampersand symbol (&) and the last four digits of your social security (e.g., Mar&1234)

3. Once you are logged in, under Access College Email click on login to student email or click on the Envelope Icon located at the top right hand side of the page.

And you’re in.
VIII- B. How to add Office365 email to your Cellphone or Ipad (Students Only)

IPad/IPhone Settings:

*Note: Before adding your Office365 email, you must set a passcode for your cellphone.*

- Settings
- Click on: Mail
- Click on: Accounts
- Click on: Add Account
- Select: Exchange
- Enter your email: (office 365 email address) e.g. NEWEMAILADDRESS@mail.ct.edu
- Description: This is Optional! You can leave this Blank or type in GCC Email so you can differentiate this mailbox from your other mailboxes.
- Click on: Next
- Enter password (Mycommnet password). Then click next.
- In the Server Field type in: outlook.office365.com
- Domain: (leave this blank)
- Username: (full NetID) e.g 01234567@student.commnet.edu
- Password: MyCommnet password
- Description: This is Optional! You can leave this Blank or type in GCC Email so you can differentiate this mailbox from your other mailboxes.
- Click on: Next
- Click on: Save

Your Gateway email account is now set up on your mobile device.

Android Settings:

- Settings
- Click on: Add account
- Select: MS Exchange
- Enter your email (office 365 email address) e.g. NEWEMAILADDRESS@mail.ct.edu
- Enter Password: MyCommnet password
- Click on: Next
- In the Server Field type in: Outlook.office365.com
- Domain: leave this blank
- Username: Type your full Netid: #######@student.commnet.edu
- Click on: Next
- Then click “Yes” on Remote Security Administration pop up.
- Sync schedule: Select Push or Automatically
- Email sync period: Select All
- Click on: Next
- Name your account
- Click: Done
- Then click: Activate.
- Click on: Activate

This is a general guide to add an email account onto Android cellphones- your settings may be slightly different.
IX- How to download Microsoft Office 365 (Student, Faculty & Staff)

1. Go to your Student Email and click this button in the top-left:

![Office Outlook](image1.jpg)

2. Click on the Office 365 link that comes up:

![Office 365 Link](image2.jpg)

3. Click on the dropdown menu labeled Install Office and click Office 365 Apps:

![Install Office Dropdown](image3.jpg)
4. Once clicked this prompt will pop-up, just click **Save File** or **Run** if it gives you the option:

![Image of a pop-up window with options to save or run the file]

5. If you had to save the file, go to your browser’s download folder and run the file you just downloaded.

![Image of the Windows Explorer window showing the Downloads folder with the file highlighted]
6. Once the installer finishes open Microsoft Word 2016 by going to the start menu and typing in ‘word’

![Microsoft Word 2016](image)

7. Open a blank document and click on the Sign In link near the top-right of the screen, and then log in. When it asks for your email type, your full NetID account a security-warning window will pop up asking for permissions, just hit yes both times and login with your NetID and Password.

![Login Portal](image)
X- How to Setup your OneDrive for Business

1. Click on the Start Button, Scroll down to find OneDrive for Business

2. Click the button that says Sync Now
3. Getting things ready to sync...

4. Your files will start syncing
How to Access Class Roster (Faculty Only)

1. Log into to [http://my.commnet.edu](http://my.commnet.edu)

2. Under Access Banner Self-Service click on **Banner Student & Faculty Self-Service**

**Note:** If you have records at multiple schools, you must first select your current school
3. On the main menu click on **Faculty/Advisor Services**

4. Click anywhere inside the **Class Lists & Roster** sub-menu to expand the section and see more choices. (If you click again, the sub-menu will collapse.)

5. Choose from **Detail Class List** or **Printable/downloadable Class Roster**.
1. If you click Detail Class List:

- Select a term from the drop-down list and click Submit.
- You will be sent to a new window. Select a course from a List or directly enter a CRN. Click Submit.
- If you need a roster for a course in a different term, click Faculty/Advisor Services to return to the main menu, click Term Selection from the sub-menu choices to select a different term, then click Class Lists & Roster.

2. If you click Printable/downloadable Class Roster:

- You will see a button labeled Spreadsheet beneath the last name on your roster.
- If you are trying to print the roster from the Banner Self-Service page, you may need to adjust your browser settings. Link here for information on printing.
- If you need a roster for a course in a different term, click Faculty/Advisor Services to return to the main menu, click Term Selection from the sub-menu choices to select a different term, then click Printable/downloadable Class Roster.
XII- How to Input Midterm and Final Grades (Faculty Only)

1. Log into [http://my.commnet.edu](http://my.commnet.edu)

2. Under Access Banner Self-Service (click on the icon or the link to Banner Self-Service on the Home page).

3. If you have records at multiple colleges, you will first be prompted to select your current college, before the main menu is displayed.

4. On the main menu, click the Faculty/Advisor Services button.

5. Click on Grading Students.
6. This will display a sub-menu where you can enter either Midterm (not all colleges enter Midterm grades) or Final Grades. **If you are not seeing the sub-menu** make sure to use the scroll bar on the right hand side of the web.

7. Select Enter Final Grades (the same process is used to enter Midterm grades, but not all colleges post midterm grades.)
8. Select the appropriate term from the list by clicking the dropdown arrow, and then click Submit.

![Select Term](image1.png)

9. Select the course you wish to access and then click submit.

![Select CRN](image2.png)

10. Once you have accessed the desired course section, enter your final grades using the drop-down menu. **If you are not seeing the grading area,** make sure to use the scroll bar on the right hand side of the web page. If you have more than 25 students in your class, you must go to the next page to finish entering grades.

**Note:**
- Registrars will have already rolled W (Withdrawals) and AUs (Audits) before they release the grade worksheet to faculty. Students who have officially withdrawn or audited a course will appear with the “W” or “AU” grade grayed out.
- **Incompletes** are handled differently at each college. Check with your Registrar’s Office for guidance.
IMPORTANT! As you are grading, make note of the message encouraging you to click the “Submit Grades” button at the bottom of the page within the 60 minute time limit for the screen.

11. Click Submit when finished.

12. Important last step! After you have entered all your grades, you should see a message on the top of the page that says “0 students to be graded.” If the message does not display “0” make sure all students have a grade assigned.
XIII- A. Protective Enclave and Multi-factor Authentication (MFA)

The Protective Enclave is a physical and/or logical separation of applications, systems and networks that process DCL3 data. The Protective Enclave provides a high security computing environment for the limited number of Faculty/Staff that process DCL3 data at the colleges and the CSCU System Office. In the past, DCL3 data was accessed from applications running directly on workstations. Now, DCL3 data must only be accessed from inside the CSCU Protective Enclave using applications launched from a virtual desktop.

The Protective Enclave will require additional security controls and restrictions to ensure the application and data remain protected. When accessing the Protective Enclave, Faculty and Staff will login through a secure channel to access to a virtual desktop. Once logged onto the virtual desktop, you will be able to access/work with DCL3 data (e.g., Banner, secure websites, documents contain confidential information, etc.). DCL3 data will not be able to leave the Protective Enclave.

The additional security controls include:

- **Multi-factor Authentication (MFA):** MFA is used to confirm your identity. It increases security by requiring you to use both something you know (e.g., your NetID and password) and something you have (e.g., a work phone or mobile device) before allowing access. This makes it more difficult for an unauthorized person to authenticate as you (i.e. they can’t get access just by knowing your password).

- **Data Loss Prevention (DLP):** DLP prevents sensitive data from leaving the Protective Enclave. If a file is saved in the Protective Enclave’s transfer share (the location where files to be transferred out of the Protective Enclave are located) that is found to contain sensitive data, it will be encrypted and therefore will not be accessible outside the Protective Enclave.

The additional restrictions include:

- **Printing:** Printers that are available from inside the Protective Enclave differ from that of standard network printers because they are protected by the boundaries of the Protective Enclave. Because of the sensitive nature of the documents being printed and the printer’s location, Faculty/Staff are assigned to only be able to print to specific Protective Enclave printers.

- **File shares:** Faculty/Staff have access to different file shares when working from within the Protective Enclave. DCL3 file shares are used to save documents/files containing DCL3 data and is available only from within the Protective Enclave. A transfer file share is available from both within the Protective Enclave and from outside the Protective Enclave as a temporary area for transferring files into and out of the Protective Enclave. It is securely shredded every night at 2AM and will not be backed up. Recovery is not possible once the secure shred has shredded documents. The Transfer file share is protected by data loss prevention (DLP) controls that do not allow documents flagged as containing DCL3 data to leave the Protective Enclave.

- **E-mail:** Access to E-mail is not allowed from inside the Protective Enclave. Faculty/Staff will need to transfer files that do not contain DCL3 data, out of the Protective Enclave in order to send the files via E-mail.

- **Inactivity timeouts:** There is a 15 minute inactivity timeout for the Protective Enclave. It is similar to a Windows screen saver, where you need to re-enter your password to get back into the Protective Enclave.
How to Access the Protective Enclave

Go to: https://enclave.ct.edu

Login with your Net ID and Password. **(Note: Before you login to Enclave you have to first set up your Multi-Factor Authentication to set your Pin Number).**

Once you login the page will look like this.
Click on **Protective Enclave Desktop**

It will redirect you to the Protective Enclave Desktop.
Click: **OK**
Before you can use the Protective Enclave

- You will first need to be granted access to the Protective Enclave. Work with the Protective Enclave Liaison to have this access granted for you.
- You will receive an email from CSCU-Authentication-noreply with a link to the MFA documentation when your account is ready to be configured. You only need to go to the MFA site when you initially configure your settings and when you need to make any changes to how you log in.

Set Up Multi-Factor Authentication (MFA)

Multi-factor Authentication is used to confirm your identity before allowing access to a service (e.g., Protective Enclave). It increases security by requiring you to use both something you know (e.g., your NetID and password) and something you have (e.g., a work phone or mobile device) to make it more difficult for an unauthorized person to authenticate as you (i.e. they cannot get access just by knowing your password).

We highly suggest you first setup your account using the "phone call" method - even if you want to use the mobile app or text message methods. This allows you to configure a backup phone number and your security questions easily. Then, if you wish to use the mobile app or the text message method after you have MFA setup to use the phone call method, change your MFA settings to use another method. The following procedure will guide you through the one-time MFA account configuration steps. Once you have configured your MFA settings following the steps below, the authentication method you choose (phone call, text message, mobile app) will be used when you attempt to login to a service that uses MFA for authentication (e.g. Protective Enclave). You cannot login to a service that uses MFA without first configuring your MFA settings.

At any time, you can change your MFA settings if you decide later that you would rather authenticate using one of the other methods or if you have forgotten your PIN or do not have your device with you, (e.g. you forgot your mobile device at home and need to change your MFA setting so you can authenticate).

You will be selecting and then configuring one of the authentication methods that you want to use (i.e. Phone, Text or app) followed by selecting and entering your Security Question information.

1. You will know your account is ready to be configured when you receive an email from CSCU-Authentication letting you know that you need to complete the MFA setup.
2. After receiving the automated e-mail, you will need to access the MFA User Portal: [https://mfa.ct.edu](https://mfa.ct.edu)
   You only need to go to the MFA User Portal to setup or change your authentication settings. After you have initially completed the setup of your MFA account, you will login directly to the service you want to access (e.g., Protective Enclave) and it will use your MFA settings to authenticate that it is you logging in.
3. Enter the following information, then click Log On:
   - **Username:** Enter your NetID (e.g. 98765432@gwcc.commnet.edu).
   - **Password:** Enter your password (Is the same password you use to login to My CommNet).

Page should look like this.
Once you login. Click the **Method** dropdown to select the authentication method you would like to configure for MFA:

The available methods are as follows:

- **Phone Call** - Calls you at a pre-defined phone number, requiring you to enter your predefined PIN on the phone keypad
- **Text Message** - Sends a text message to a pre-defined phone number with an authorization code, requiring you to reply to the text message with the code and your predefined PIN
- **Mobile App** - Uses the Microsoft Authenticator App (Windows Phone, Android, or iOS only)

**Phone Call**

If you select the **Phone Call** method, you are setting up your MFA authentication to call you when you want to authenticate. It is recommended to use a mobile phone that you always have with you, so you can authenticate no matter where you are located. You will need to be able to access the phone during configuration. You will also enter a backup phone number that will be used if the first phone number is not answered or goes to voicemail.

1. In the **Phone** text box, type in a primary and a backup phone number (including area code) that you would like the Microsoft authentication servers to call you on. In the **PIN** and **Confirm PIN** text boxes, type in a PIN of your choice which will be asked of you during the authentication process, then click **Call Me Now to Authenticate**:
2. Within 30 seconds of clicking "Call Me Now to Authenticate", you will receive an automated phone call from Microsoft's authentication servers. You will then be asked to enter your PIN followed by the # key to complete the authentication process.

3. Continue to Completing the Setup Process to configure your security questions and answers. If you do not configure your security questions and answers, the setup of MFA will not be complete and you will need to complete your setup again.

Text Message
When you select the Text Message method, you are setting up your MFA authentication to text you when you want to authenticate. It is recommended to use a mobile phone that you always have with you, so you can authenticate no matter where you are located. You will need to be able to access the text message during configuration. NOTE: For the purpose of this document, the iOS platform will be used as an example.

1. In the Phone text box, type in the phone number (including area code) of a mobile device that is capable of receiving text messages (text message rates apply) that you would like the Microsoft authentication servers to send the text message to. In the PIN and Confirm PIN text boxes, type in a 4 digit PIN of your choice which will be asked of you during the authentication process, then click Text Me Now to Authenticate:
2. Within 30 seconds, you will receive a text message from Microsoft’s authentication servers (the phone number will not be the same each time) with a one-time use verification code, similar to what is shown below. Reply to the text with the code you received followed by your PIN.

![Text Message](image)

NOTE: You can enter the code followed by the PIN with no spaces in between or with a space or a + in between as well. For example all these are acceptable (9522086756 or 952208 6756 or 952208+6756)

3. Since this passcode is used only once, once you've replied, you do not need to save the text message. The next time you authenticate using MFA, you will receive a different passcode that you will need to reply to in order to authenticate. NOTE: You will also see the name of the service you are requesting access to also displayed in the text message. The above text was sent in response to a login attempt on the MFA User Portal. When you login to the Protective Enclave, you will see "Reply with this code + your PIN for Netscaler PE SNIP verification" indicating it is for access to the Protective Enclave.

4. Continue to [Completing the Setup Process](#) to configure your security questions and answers. If you do not configure your security questions and answers, the setup of MFA will not be complete and you will need to complete your setup again.

**Mobile App**

When you select the Mobile App method, you are setting up your MFA authentication to use the Microsoft Authenticator app when you want to authenticate. In order to use this method, you must first have the Microsoft Authenticator app for Windows Phone, Android, or iOS installed on your mobile device and enabled for push notifications.
**IMPORTANT NOTE:** There are varieties of “authenticator” apps (e.g., Google Authenticator). You must use the Microsoft Authenticator app to authenticate.

You can download the Microsoft Authenticator app by selecting the appropriate operating system for your mobile device:

### Apple iOS
![Microsoft Authenticator app on Apple iOS](image)

### Android
![Microsoft Authenticator app on Android](image)

For the purpose of this document, the iOS platform will be used as an example.

1. Once you have the **Microsoft Authenticator** app installed, open the Microsoft Authenticator app on your mobile device. The first time you open the app, you may be prompted with **“Authenticator” Would Like to Send You Notifications**, similar to what is shown below:

![Authenticator notification](image)

If prompted, tap **Allow**; otherwise, tap the **plus (+) symbol** or **Add account**. NOTE: You may have other accounts configured that you use Microsoft Authenticator app to authenticate with that will be listed or the list may be empty if this is the first time using the Microsoft Authenticator app:
2. Tap the **Work or school account** option:

The QR code scanner will launch on the app. The first time you open the app, you may be prompted with "**Authenticator** Would Like to Access the Camera", tap **OK** as you will need to scan the QR code using your mobile phone's camera:

3. On the **Multi-Factor Authentication User Setup** screen, click **Generate Activation Code**:
4. You will be presented with an activation code (QR Code) and URL as shown below:

Multi-Factor Authentication User Setup

Follow the instructions below to activate the Microsoft Authenticator app on your phone and test an authentication using the mobile app.

Enter the following activation code and URL when prompted by the mobile app. The activation code expires in 10 minutes. You may generate a new code at any time.

Activation Code

URL

https://mfa.ct.edu/app

Generate New Activation Code

PIN

Confirm PIN

After activation is complete, click the following button to test authentication and continue the setup process.

Authenticate Me Now  Cancel
5. Scan the QR code using the Microsoft Authenticator app from your mobile device. It doesn't have to be exactly lined up in the green square, the app will be able to recognize the QR code and will add the account:

6. Once scanned and the code is accepted, the account will be added to the list of accounts:
7. In the PIN and Confirm PIN text boxes, type in a 4 digit PIN of your choice which will be asked of you during the authentication process on your mobile device and click **Authenticate Me Now:**

Multi-Factor Authentication User Setup

Follow the instructions below to activate the Microsoft Authenticator app on your phone and test an authentication using the mobile app.

Enter the following activation code and URL when prompted by the mobile app. The activation code expires in 10 minutes. You may generate a new code at any time.

Activation Code

![QR code](https://mfa.ct.edu/app)

URL

https://mfa.ct.edu/app

PIN

· · · ·

Confirm PIN

· · · ·

After activation is complete, click the following button to test authentication and continue the setup process.
8. Within 30 seconds, your Microsoft Authenticator app will prompt you to approve sign-in. Type in the PIN you selected from the previous step and tap Approve:

NOTE: If the Microsoft Authenticator app didn't prompt you to approve, be sure that you have allowed push notifications from the Microsoft Authenticator app on your mobile device.

If using an iOS device with Touch ID enabled, you may see that Touch ID Set Up was automatically done for you so you can use your fingerprint to authenticate instead of the PIN, tap OK:
9. Continue to Completing the Setup Process to configure your security questions and answers.

If you do not configure your security questions and answers, the setup of MFA will not be complete and you will need to complete your setup again and may need to delete the account you just created in the Microsoft Authenticator app and start again by rescanning another QR code.

Completing the Setup Process

1. Select and complete your security questions and answers and click **Continue**:

   **Security Questions**

   Please choose security questions and answers before continuing. These questions will be used to validate your identity should you need support using Multi-Factor Authentication.

   - **Question 1**
     - What was your high school mascot?
     - Answer

   - **Question 2**
     - What was your favorite pet's name?
     - Answer

   - **Question 3**
     - What is your favorite movie?
     - Answer

   - **Question 4**
     - What was your favorite teacher’s name?
     - Answer

   ![Continue and Cancel buttons](image)
2. Once you have completed your questions and answers, you will be taken to the **Welcome** screen:

3. Before logging out of the MFA User Portal, it is **strongly** recommended that you add a phone number as a backup method of authenticating if your primary method is unavailable by following the instructions for **Changing Phone**. If your primary method is Phone Call, you may enter a **BACKUP Phone Number** that will be used if you cannot be reached on the primary phone number.
XIII- B. How to Change your Multi-Factor Authentication (MFA) Settings

The following procedures will guide you through changing any of the following MFA settings on your account:

- Changing your Authentication Method
- Changing or Adding a Phone number
- Changing your PIN
- Activating the Mobile App

Changing the Authentication Method

The following procedure will guide you through changing the authentication method associated with your MFA account. Perform the following steps to change your current method:

1. First, log into MFA User Portal [https://mfa.ct.edu](https://mfa.ct.edu)
2. From the navigation menu on the left side of the window, select **Change Method**:

3. Click the **Method** dropdown and select the method you'd prefer to use for MFA (see figures below):

   **Selecting MFA Method**
Then

The available methods are as follows:

- **Phone Call** - Calls you at a pre-defined phone number, requiring you to enter an expected response on the phone keypad
- **Text Message** - Sends a text message to a pre-defined phone number with an authorization code, requiring you to reply to the text message
- **Mobile App** - Uses the Microsoft Authenticator App (Windows Phone, Android, or iOS only)

4. **Click Save:**

Once your method has been saved, you will see a message similar to what is shown below:

If you received the above message, your method has been changed and that method will now be used when authenticating using MFA. You may **Log Off**.
NOTE: If you receive any of the following error messages after clicking Save, click the link next to the error message to correct the issue and then repeat that procedure:

**Phone Call** - You must specify a phone number for your account before you can change your method to Phone Call. Click the Change Phone link in the navigation menu to specify a phone number.

**Text Message** - You must specify a phone number for your account before you can change your method to Text Message. Click the Change Phone link in the navigation menu to specify a phone number.

**Mobile App** - You must activate the Microsoft Authenticator mobile app before you can change your method to Mobile App. Click the Activate Mobile App link in the navigation menu to begin your activation.

### Changing or Adding a Phone number

The following procedure will guide you through changing the phone number(s) associated with your MFA account or adding a Backup phone number:

1. First, log into MFA User Portal ([https://mfa.ct.edu](https://mfa.ct.edu))
2. From the navigation menu on the left side of the window, select Change Phone:
3. Depending on your current MFA method, you will have a choice to enter one or two phone numbers:

**Text Message or Mobile App Method:**

My Account: Change Phone

Specify a new phone number to call for Multi-Factor Authentication.

**New Phone Number**

United States & Canada +1

Save

**Phone Call Method:**

My Account: Change Phone

Specify a new phone number to call for Multi-Factor Authentication.

**PRIMARY**

New Phone Number

United States & Canada +1

New Extension

**BACKUP**

New Phone Number

United States & Canada +1

New Extension

Save
In the **New Phone Number** text box(es), type in the phone number(s) (including area code) that you would like the Microsoft authentication servers to call or text you on and click **Save**.

4. Once your Phone has been changed, you will see a message similar to what's shown below:

**Change Phone Success**

![Change Phone Success](image)

5. That completes the procedure for changing the phone number(s) associated with your MFA account.

**Changing your PIN**

The following procedure will guide you through changing the PIN used when authenticating with your MFA account:

1. First, log into MFA User Portal ([https://mfa.ct.edu](https://mfa.ct.edu))
2. From the navigation menu on the left side of the window, select **Change PIN**.
3. In the **New PIN** and **Confirm PIN** text boxes, type in a 4 digit PIN of your choice which will be asked of you during the authentication process on your mobile device and click **Save**. You will not be able to see your old PIN, but can set a new PIN to use:

![My Account: Change PIN](image)

4. Once your PIN has been changed, you will see a message similar to what’s shown below:

![Your PIN has been changed](image)

That completes the procedure for changing the PIN associated with your MFA account.
XIII- C. How to Activate the Mobile App

Before you can select the Mobile App method, you must first activate the mobile app with your mobile device. When using the Mobile App method, you will receive a push notification from the Microsoft Authenticator app to approve your authentication. In order to use this method, you must first have the Microsoft Authenticator app for Windows Phone, Android, or iOS installed on your mobile device and enabled for push notifications.

**IMPORTANT NOTE:** There are varieties of "authenticator" apps (e.g., Google Authenticator). You must use the Microsoft Authenticator app to authenticate.

You can download the Microsoft Authenticator app by selecting the appropriate operating system for your mobile device:

**Apple iOS**

![Microsoft Authenticator App for Apple iOS](image)

**Android**

![Microsoft Authenticator App for Android](image)

For the purpose of this document, the iOS platform will be used as an example. The following procedure will guide you through the steps to Activate Mobile App and PIN associated with your MFA account:

1. First, log into MFA User Portal ([https://mfa.ct.edu](https://mfa.ct.edu))
2. Once you have the Microsoft Authenticator app installed, from the navigation menu on the left side of the window, select **Activate Mobile App**:
3. Open the **Microsoft Authenticator** app on your mobile device. The first time you open the app, you may be prompted with "**Authenticator** Would Like to Send You Notifications," similar to what is shown below:

![Notification Prompt](image)

If prompted, tap **Allow**; otherwise, tap the **plus (+) symbol** or **Add account**. NOTE: You may have other accounts configured that you use Microsoft Authenticator app to authenticate with that will be listed or the list may be empty if this is the first time using the Microsoft Authenticator app:

![Add Account](image)
4. Tap the **Work or school account** option:

The QR code scanner will launch on the app. The first time you open the app, you may be prompted with "Authenticator" Would Like to Access the Camera, tap OK as you will need to scan the QR code using your mobile phone's camera:

5. On the **My Account: Activate Mobile App** screen, click **Generate Activation Code**:

**My Account: Activate Mobile App**

First install the Microsoft Authenticator mobile app on your phone, then click the Generate button to receive an activation code. The activation code will be entered in the mobile app to complete the activation process. The activation code expires in 10 minutes. You may generate a new code at any time.
6. You will be presented with an activation (QR) code and URL as shown below:

![QR Code and Activation Code](image)

- **Activation Code**: [Redacted]
- **URL**: https://mfa.ct.edu/app

7. Scan the QR code using the Microsoft Authenticator app from your mobile device. It doesn’t have to be exactly lined up in the green square, the app will be able to recognize the QR code and will add the account:
8. Once scanned and the code is accepted, the account will be added to the list of accounts:

![Image of mobile app account](image)

Your Mobile App is now activated on your mobile device. Before you will be able to authenticate using the Mobile App method, you will also need to make sure you have a PIN set. Please following the instructions for Changing PIN before logging off.
XIV- A. Campus Wireless Access

Gateway Community College has established a wireless access system to provide students, faculty, and staff access to internet services. This provides the same experience as using a broadband service from home.

The ConnSCU Internet – wireless network is broadcast throughout the downtown campus in public areas of the campus and needs little configuration to use.

In order to connect, the user must have a valid NetID account (generated automatically for students, faculty, and staff - the same username and password used to log into college computer labs), a personal computer with up-to-date virus protection and patches, and a wireless card that is configured and functioning properly with its operating system.

Computer Requirements

Operating systems- Preferred: Windows XP, Windows 7 or 8, 10, Mac OS X 10.6 or later

Supported Browsers- Internet Explorer 8-11, MS Edge, Mozilla Firefox, Safari.

Your computer must have a functioning wireless internet card (wireless G or N preferred).

In all of the following guides, - These Screen Shots are example of what you will see- In some instances your screens will be slightly different.

Windows Wi-Fi Access Instructions

1. Click on the Wireless icon

2. There may be a few wireless networks that may be visible in the “Wireless network screen”. The Gateway wireless network is identified as ConnSCU.
3. Click on this selection and then click the Connect button.

![Image](image1.png)

4. The following pop-up will be displayed

![Image](image2.png)

5. Then it will open a new window that it will look like this. In here you will type in your username & password, the same way you login into the campus computer.

![Image](image3.png)

Then click: OK

Upon sucessfully entering your NetID and password, you will then see Windows Security Alert Pop Up

6. Click on: **Connect** and you can now navigate in the internet.

![Image](image4.png)
XIV- B. Mac OS Wi-Fi Access Instructions

1. Click on: the Wi-Fi

2. Then click on: **ConnSCU**

3. It will pop up a window asking for your credentials, type in your Net ID and password the same way you login to the campus computer, and then click ok.

3. Upon successfully entering your NetID and password, you can now navigate in the internet.
XIV- C. How to connect to the Wi-Fi using your IPhone & IPad (Students, Faculty & Staff)

First you will Click on: Settings

The Setting page will look like this.

In here you will turn on the Wi-Fi

Once you turn on, the page will look like this.
In here you will see all the networks available

Then you will see a message next to Wi-Fi saying Not Connected

You will then click on ConnSCU.
Once you click on: **ConnSCU**

It will open a new window that it will look like this.

In here you will type in your NetID & Password, the same way you login into the campus computer.

Then click: **Join**

Once done it will open a certificate page that looks like this.

Click: **Trust** - You can now navigate in the internet.
XIV- D. How to Access the Wi-Fi using your IPhone, IPad and Android (Faculty & Staff Only)

Instructions for Iphone

1. First you will Click on: Settings.
2. Turn on the Wi-Fi. Once you turn on the Wi-Fi, you will see all the networks available.
3. You will then click on: ConnSCU.
4. Once you click ConnSCU, It will open a new window asking for username & password.
5. Under Username type in your NetID (01234567@gwcc.commnet.edu). For Password type the same password you used to login into the campus computer.
6. Click: Join, then It will open a certificate page, click Trust.
- You can now navigate in the internet.

Instructions for Android

1. Click on Settings
2. Select on Wi-Fi
3. Turn On the Wi-Fi
4. Select ConnSCU
5. In Authentication Select PEAP
6. On Secondary Authentication Select: MSCHAPV2
7. On Certificate Select: Do not Validate
8. Under Identity type in your NetID (01234567@gwcc.commnet.edu).
9. Anonymous Identity: Leave this Blank
10. For Password type the same password you used to login into the campus computer.
11. Then click: Connect