Citrix Virtual Machines for MSBA

Fall 2018: How To Begin Guide

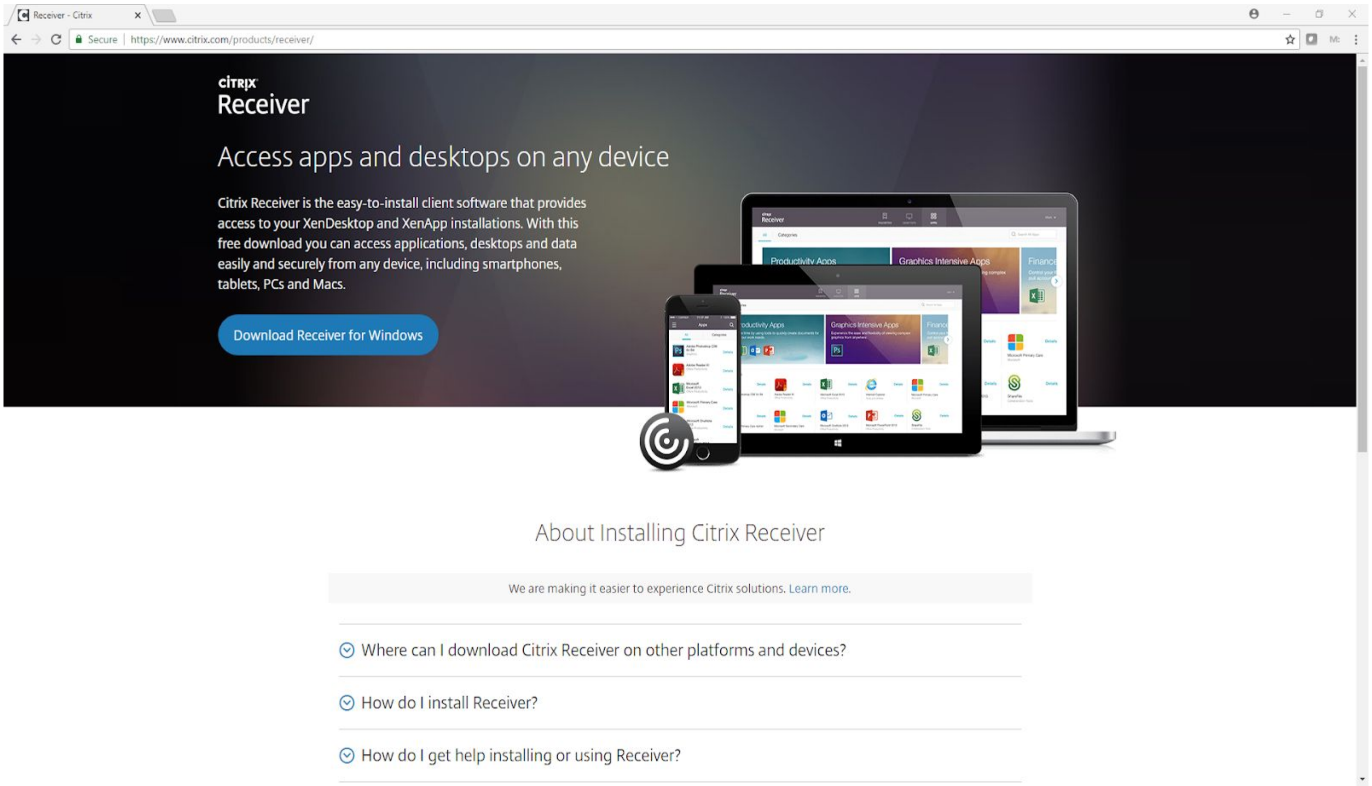
University of Minnesota
Driven to Discover℠

Install Citrix Receiver

To use the Citrix virtual machines provisioned for you, you will need to download "Citrix Receiver." This client is a lightweight application that allows you to access Citrix resources. It can be found by visiting:

https://www.citrix.com/products/receiver/

When downloaded, please run the installer and use default settings.


Receiver - Citrix
Secure | https://www.citrix.com/products/receiver/

citrix Receiver

Access apps and desktops on any device

Citrix Receiver is the easy-to-install client software that provides access to your XenDesktop and XenApp installations. With this free download you can access applications, desktops and data easily and securely from any device, including smartphones, tablets, PCs and Macs.

Download Receiver for Windows

About Installing Citrix Receiver

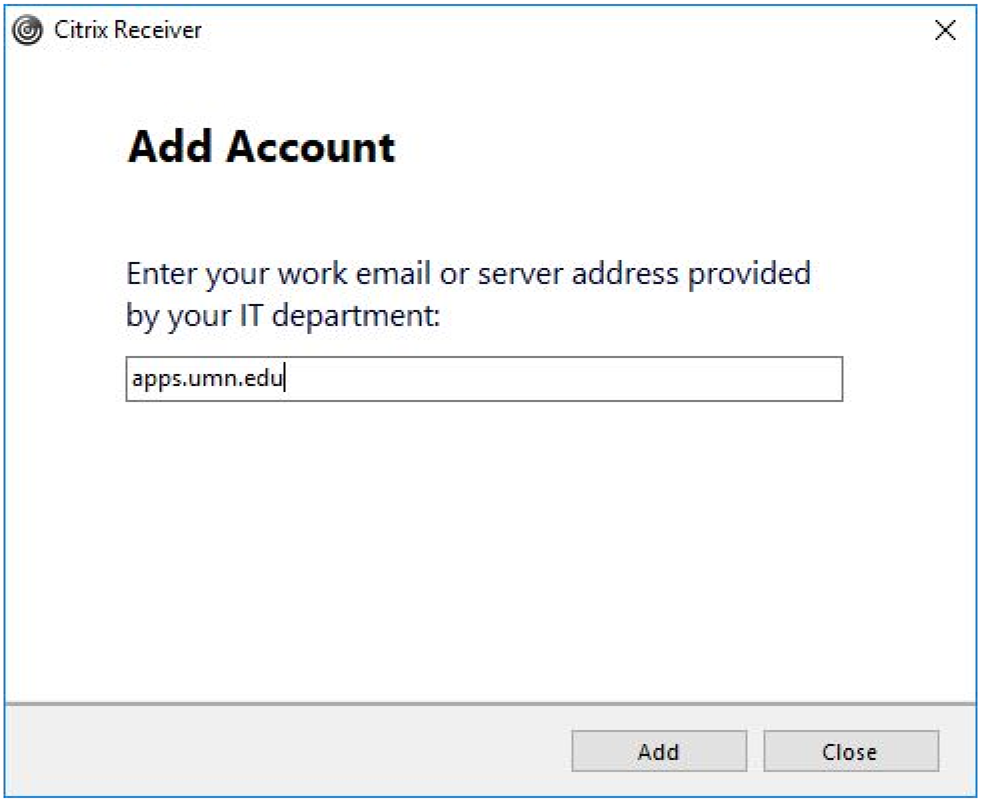
We are making it easier to experience Citrix solutions. Learn more.

- Where can I download Citrix Receiver on other platforms and devices?
- How do I install Receiver?
- How do I get help installing or using Receiver?

Note: When visiting the Citrix Receiver download site, it will automatically detect your OS and will provide the link to download the appropriate version.

Configure Citrix Receiver

When Citrix Receiver has been installed, you can run the application by selecting “Citrix Receiver” from the start menu on Windows or in your launchpad if using MacOS. One of the first screens you will see is shown below:



Citrix Receiver

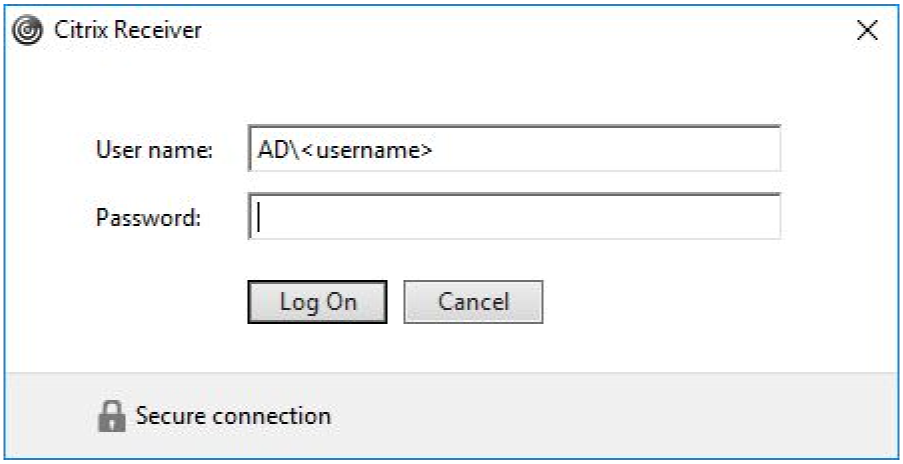
Add Account

Enter your work email or server address provided by your IT department:

apps.umn.edu

You’ll need to enter “apps.umn.edu” as the server address, then click “Add.”

The next window will prompt you for your login information:



Citrix Receiver

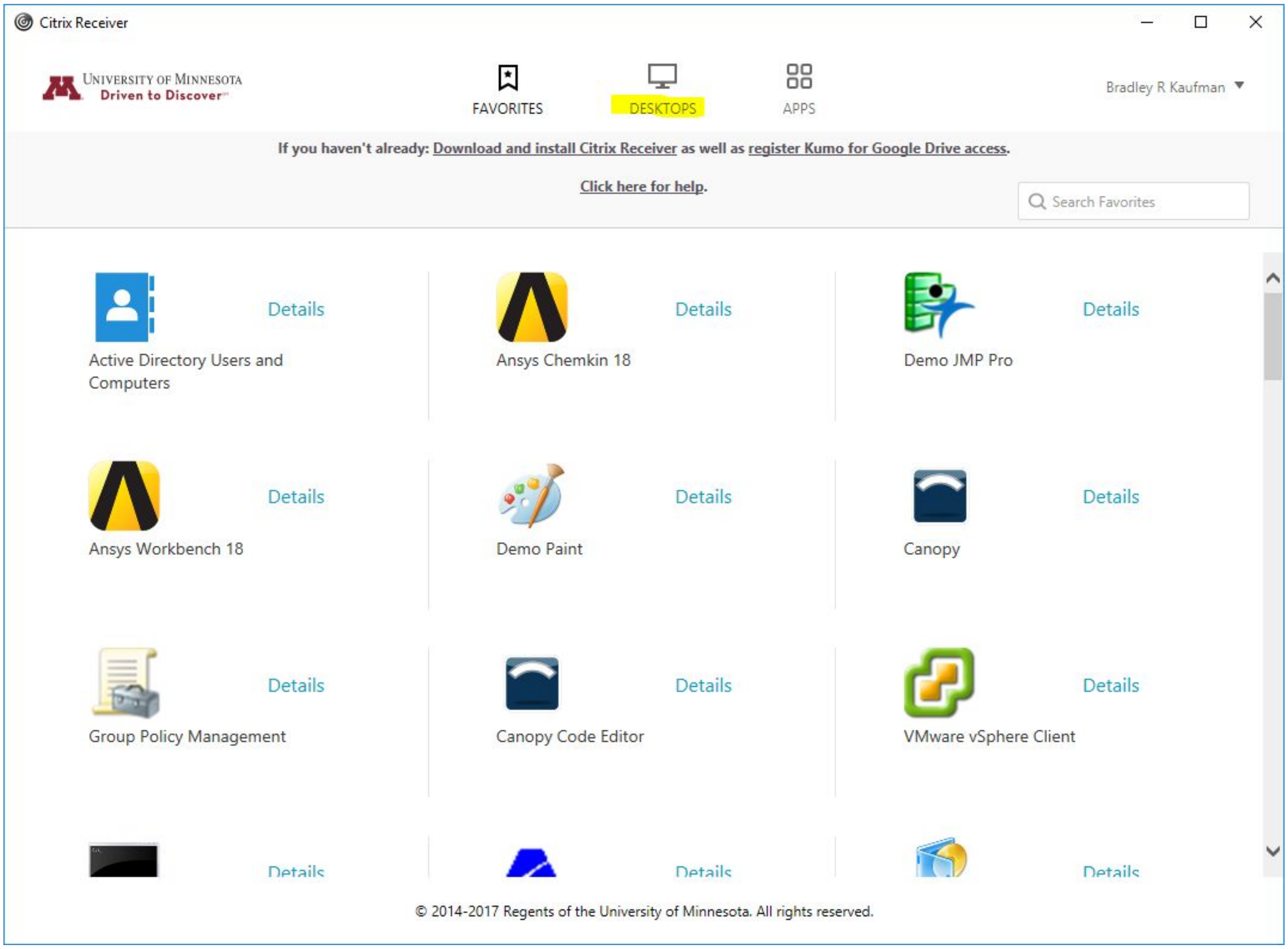
User name: AD\<username>

Password:

Use your University X.500 username and password. As shown above, please prepend your username with “AD\” -- this is not required but ensures the correct domain is being specified. Click “Log On” once your information has been entered.

Accessing Your Personal Virtual Machine

After you've successfully logged in, you will see a window similar to below. Select the tab at the top labeled "DESKTOPS." The other apps that show up are sample applications. You will not need them, they are simply provided as samples. Attempting to use sample applications is fine but please note that any work done on them will not be saved.

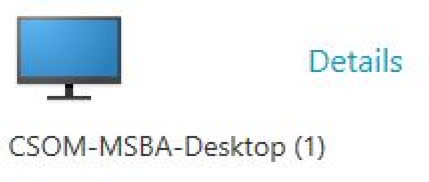


If you haven't already: Download and install Citrix Receiver as well as register Kumo for Google Drive access.

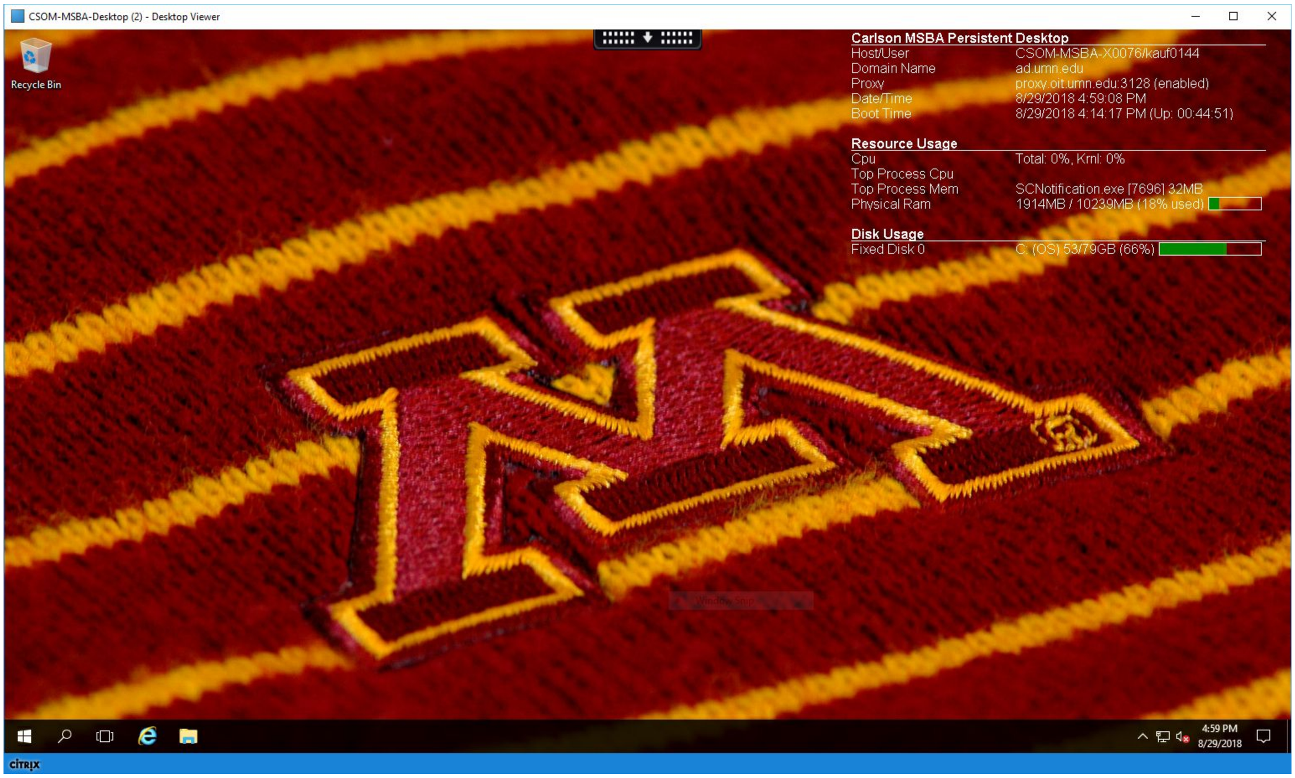
Click here for help.

© 2014-2017 Regents of the University of Minnesota. All rights reserved.

After selecting the "DESKTOPS" tab, you should see a desktop with a name similar to:



When you click it, it should bring up your Citrix Desktop Viewer window, which will open your virtual machine.



```
Carlson MSBA Persistent Desktop
Host/User              CSOM-MSBA-X0076/kauf0144
Domain Name            ad.umn.edu
Proxy                  proxy.oit.umn.edu:3128 (enabled)
Date/Time              8/29/2018 4:59:08 PM
Boot Time              8/29/2018 4:14:17 PM (Up: 00:44:51)

Resource Usage
Cpu                    Total: 0%, Krnl: 0%
Top Process Cpu
Top Process Mem        SCNotification.exe [7696] 32MB
Physical Ram           1914MB / 10239MB (18% used)

Disk Usage
Fixed Disk 0           C: (OS) 53/79GB (66%)
```

Using Your Personal Virtual Machine

Applications Currently Available:

- RStudio / R
- Cloudera VM via Vagrant and Oracle VirtualBox
- Anaconda 3
- Google Chrome (for Canvas/Moodle access only!)
- Microsoft Office

Data

Any files you need to save should be saved to your "My Documents" folder. Your desktop has ample storage space, but storage is limited so requests for additional storage will not be fulfilled. Please be good stewards of University storage resources…meaning do not use more than you absolutely need to. Please do not use more than 10 GB of space in your "My Documents" folder. Any files saved outside of "My Documents" **WILL NOT** be saved in the event your virtual desktop needs to be rebuilt.

Monthly Updates

To maintain the integrity of the operating system on each of these desktops, they are patched every Saturday morning during the weekend of the first Sunday of the month. You can work on the virtual machine during this time but please know to save because the machine will reboot during this time.

Fall 2018 Schedule: 9/1/2018, 10/6/2018, 11/3/2018, 12/1/2018 Between 5:00 AM and 12:00 PM

If your virtual machine is unavailable for more than an hour during these times, please submit a support request.

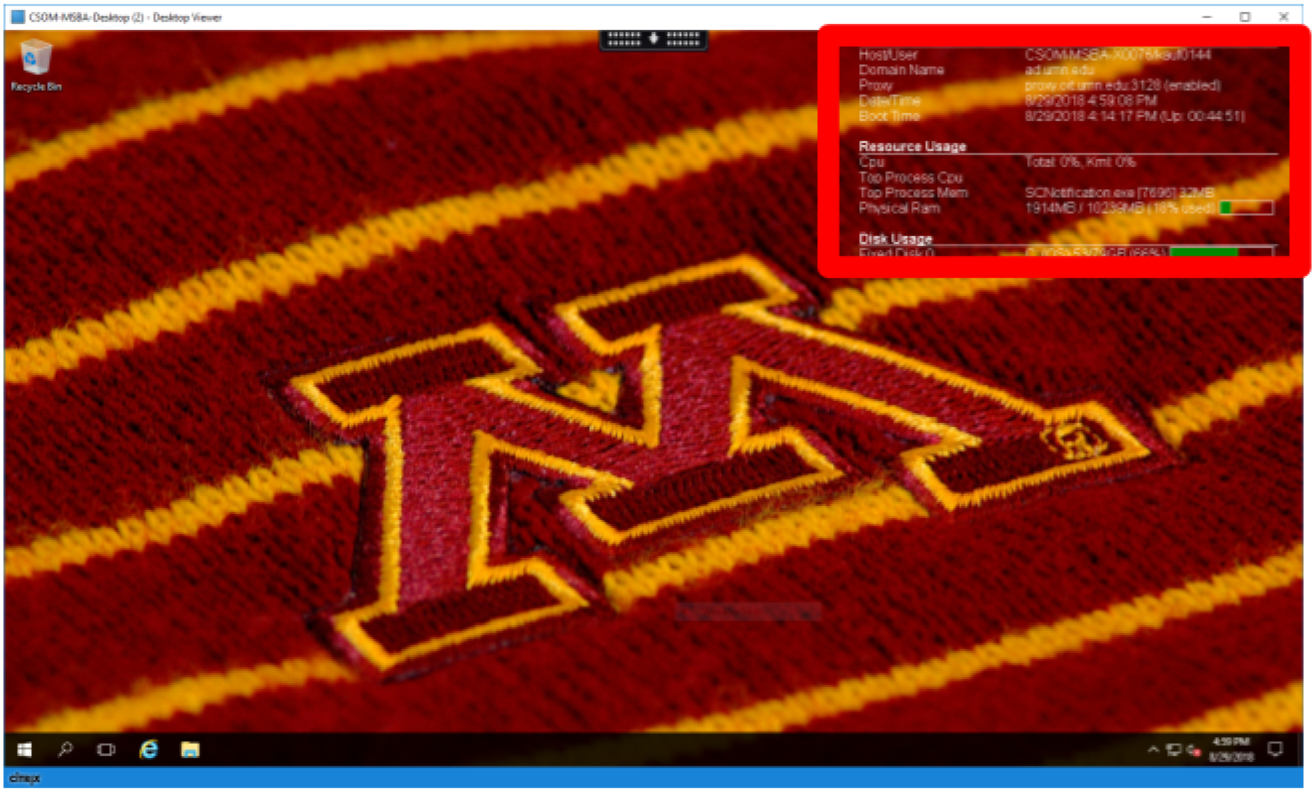
Software Installation

Software installation of any kind is prohibited on these desktops without the approval of your instructor or CSOM-IT. Exceptions to this rule would be python packages or R packages.

Resource Usage:

There may be times when you have larger data sets to process or have an open process that may be resource intensive. During this time, it is a good idea to monitor resource consumption using two tools:

At a Glance:

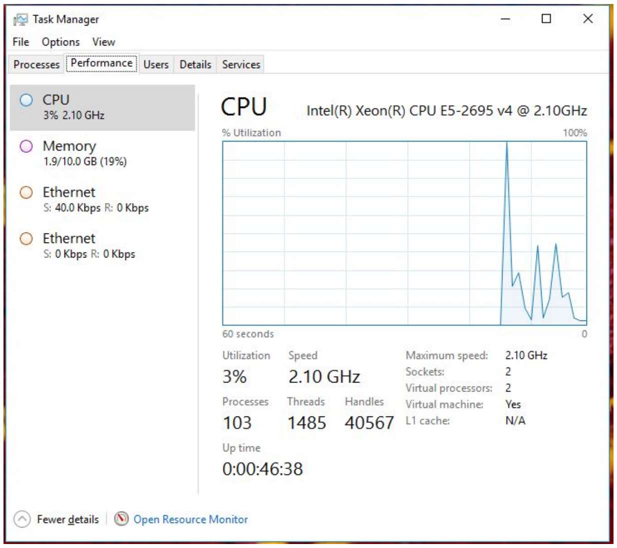


```
Host/User            CSOM-MSBA-X0076\kaul0144
Domain Name          ad.umn.edu
Proxy                proxy.oit.umn.edu:3128 (enabled)
Date/Time            8/29/2018 4:59:08 PM
Boot Time            8/29/2018 4:14:17 PM (Up: 00:44:51)

Resource Usage
Cpu                  Total: 0%, Krnl: 0%
Top Process Cpu
Top Process Mem      SCNotification.exe [7696] 32MB
Physical Ram         1914MB / 10239MB (18% used)

Disk Usage
Fixed Disk 0         C:\ [illegible] GB (66%)
```

Task Manager:



```
CPU
3% 2.10 GHz
Memory
1.9/10.0 GB (19%)
Ethernet
S: 40.0 Kbps R: 0 Kbps
Ethernet
S: 0 Kbps R: 0 Kbps

CPU    Intel(R) Xeon(R) CPU E5-2695 v4 @ 2.10GHz

Utilization   Speed                 Maximum speed:       2.10 GHz
3%            2.10 GHz              Sockets:             2
                                    Virtual processors:  2
Processes     Threads    Handles    Virtual machine:     Yes
103           1485       40567      L1 cache:            N/A

Up time
0:00:46:38
```

Information from both of the sources above will also be helpful if you need to submit a support request to csommsbahelp@umn.edu. It includes information about CPU, RAM, and storage usage, along with basic information about your virtual machine including name, proxy status, etc.

Performance

At times there may be slower performance due to load being placed on the virtualization cluster that each of these servers in provisioned on. At those times, it is important to remain patient. If performance degradation is persistent or if your virtual machine is not responsive, please send a request to csommsbahelp@umn.edu.

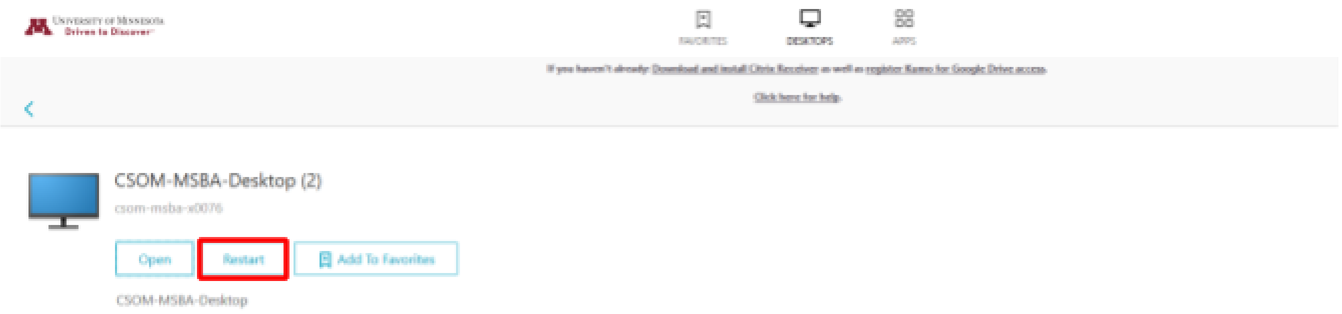
Browser Usage

Browser usage should be limited to accessing course and University resources only. Please do not open attachments from unknown senders if you open your UMN Gmail. If you are browsing to external sites and become infected, your machine will be deleted and will need to be restored to its original configuration. Your data will not be saved and will be lost if this occurs.

Support

If you need assistance with a problem using software for a specific course, please consult with your instructor. If you are having issues logging in, if applications will not run, or if you have another technical question unrelated to your course content but pertains to these virtual machines, please submit a ticket to csommsbahelp@umn.edu and someone from Carlson School IT will assist.

If your virtual machine is not responsive or you cannot login, restarting your virtual desktop will typically resolve the problem. You can do this by browsing to your desktop on apps.umn.edu or within Citrix Receiver and selecting “Restart” … this process takes a few minutes to complete, so please wait before trying to login again.



If you haven't already: Download and install Citrix Receiver as well as register Kamo for Google Drive access.

Click here for help.

CSOM-MSBA-Desktop (2)

csom-msba-x0076

CSOM-MSBA-Desktop

Prohibited Activity

Below is a list of prohibited activities on your virtual desktop. This list is not exhaustive but should give a good example of what type of conduct is acceptable and what is not. Each virtual machine is monitored and audited.

- Browsing the web for non-course related content
- Installing or downloading software (R and Python packages are acceptable)
- Circumventing security restrictions or controls (this includes making or attempting to make changes to the firewall, access control lists, or attempting to exploit a vulnerability)
- Attempting to access resources that belong to another student (access is monitored and audited)
- Changing configuration items of the virtual desktop
- Using the virtual desktop for anything other than course-related activity (i.e. installing or attempting a web server)
- Shutting down your virtual desktop. Restarts will be permitted.

Acceptable Use:

Please familiarize yourself with the University's Acceptable Use Agreement found at the end of this documentation. Any violation of this agreement will result in loss of access to this service and could be subject to other penalties. Your personal virtual machine is to be used specifically for class purposes and class purposes only. This means that you are not allowed to install additional software unless instructed to by your instructor. Packages for R and Python are exceptions to this, but please consult with your instructor or contact csommsbahelp@umn.edu if you intend on installing packages that are not vetted through your courses. Security measures may be put in place at certain times throughout the semester for data integrity purposes. Any attempt to circumvent security policies or any other misuse of the provisioned resources is subject to remedies listed in the Acceptable Use Agreement. You have been given privileges that allow you to do your work and explore the software provided. Any abuse of these privileges will result in them being taken away.

A Good Rule of Thumb: If you are unsure if you should be doing something, chances are you should not be. Please ask if you are unsure.

ADMINISTRATIVE POLICY

Acceptable Use of Information Technology Resources

Responsible University Officer(s):

- Vice President for Information Technology

Policy Owner(s):

- Vice President for Information Technology

Policy contact(s):

- *Brian Dahlin*

Date Revised:

Aug 13, 2015

Effective Date:

Dec 1, 1996

POLICY STATEMENT

Computers and other information technology resources are essential tools in accomplishing the University's mission. Information technology resources are valuable community assets to be used and managed responsibly to ensure their integrity, confidentiality, and availability for appropriate research, education, outreach and administrative objectives of the University of Minnesota. University community members are granted access to these resources in support of accomplishing the University's mission.

All users of University information technology resources, whether or not affiliated with the University, must follow University policies; federal, state and local laws; and contractual obligations. These include but are not limited to information security, data privacy, commercial use, and those that prohibit harassment, theft, copyright and licensing infringement, and unlawful intrusion and unethical conduct.

Units that grant guest access to information technology resources must make their guests aware of their acceptable use responsibilities.

Acceptable Use

Acceptable use includes, but is not limited to respecting the rights of other users, avoiding actions that jeopardize the integrity and security of information technology resources, and complying with all pertinent licensing and legal requirements.

Users must comply with applicable laws and regulations, contractual agreements, Board of Regents and Administrative policies, and licensing agreements.

Users must use only information technology resources they are authorized to use and only in the manner and to the extent authorized. Ability to access information technology resources does not, by itself, imply authorization to do so.

Users are responsible for protecting their University-assigned accounts and authentication (e.g., password) from unauthorized use.

Users must abide by the security controls on all information technology resources used for University business, including but not limited to mobile and computing devices, whether University or personally owned.

Users of information technology resources are responsible for the content of their personal communications and may be subject to liability resulting from that use. The University accepts no responsibility or liability for any personal or unauthorized use of its resources by users.

Unacceptable Use

Users are not permitted to share authentication details or provide access to their University accounts to anyone else.

Users must not circumvent, attempt to circumvent, or assist another in circumventing the security controls in place to protect information technology resources and data.

Users must not knowingly download or install software onto University information technology resources which may interfere or disrupt service, or does not have a clear business or academic use.

Users are prohibited from willingly engaging in activities that interfere with or disrupt network users, equipment or service; intentionally distribute viruses or other malicious code; or install software, applications, or hardware that permits unauthorized access to information technology resources.

Users must not engage in inappropriate use, including but not limited to:

- Activities that violate state or federal laws, regulations or University policies.
- Harassment.
- Widespread dissemination of unsolicited and unauthorized electronic communications.

Users must avoid excessive use of system information technology, including but not limited to network capacity. Excessive use means use that is disproportionate to that of other users, or is unrelated to academic or employment-related needs, or that interferes with other authorized uses. Units may require users to limit or refrain from certain activities in accordance with this provision.

Privacy and Security Measures

Users must not violate the privacy of other users. Technical ability to access others' accounts does not by itself imply authorization to do so.

The University takes reasonable measures to protect the privacy of its information technology resources and accounts assigned to individuals. However, the University does not guarantee absolute security and privacy. Users should be aware that any activity on information technology resources may be monitored, logged and reviewed by University-approved personnel or may be discovered in legal proceedings.

The University assigns responsibility for protecting its resources and data to system administrators, and data custodians, who treat the contents of individual assigned accounts and personal communications as private and does not examine or disclose the content except:

1. as required for system maintenance including security measures;
2. when there exists reason to believe an individual is violating the law or University policy; and/or
3. as permitted by applicable policy or law.

Employees must understand that any records and communications they create related to University business, electronic or otherwise, may be subject to disclosure under the Minnesota Government Data Practices Act on a University or personally owned device.

The University reserves the right to employ security measures. When it becomes aware of violations, either through routine system administration activities or from a complaint, it is the University's responsibility to investigate as needed or directed, and to take necessary actions to protect its resources and/or to provide information relevant to an investigation.

Enforcement

Individuals who use information technology resources to violate a University policy, law(s), contractual agreement(s), or violate an individual's rights, may be subject to limitation or termination of user privileges and appropriate disciplinary action, legal action, or both. Alleged violations will be referred to the appropriate University office or law enforcement agency.

The University may temporarily deny access to information technology resources if it appears necessary to protect the integrity, security, or continued operation of these resources or to protect itself from liability.

Individuals or units should report non-compliance with this policy to University Information Security (*abuse@umn.edu*). If you must report anonymously, use the University Ethics Point confidential reporting system.

Special Situations

Units within the University may define additional conditions of use for information technology resources or facilities under their control. Such additional conditions must be consistent with or at least as restrictive as any governing Board of Regents or Administrative policy, and may contain additional details or guidelines.