Intro to Accessing the Cluster

Introduction: This workshop will introduce users on how to remotely access the clusters and how to set up and personalize their environment for their computational needs. After the workshop, participants will understand:

- How to (remotely) access the cluster.

Participants will require an intro level of experience of using Linux, as well as the ability to use a text editor from the command line.

Course Goals:

- Introduce a number of ways to access an ARCC HPC Cluster.

Sections

Methods for HPC Cluster Access

There are a number of different ways to access the cluster, but all consist of 2 main methods for access:

OnDemand (web based):

- MedicineBow
- Beartooth
- WildIris

SSH (secure shell CLI):

- MedicineBow (Requires setup with ssh-key and certificate)
- Beartooth
- WildIris

Try it: Access HPC with OnDemand

Goals: Walk through accessing MedicineBow HPC through the OnDemand Portal.

If users have attended previous workshops, this will be review.

---

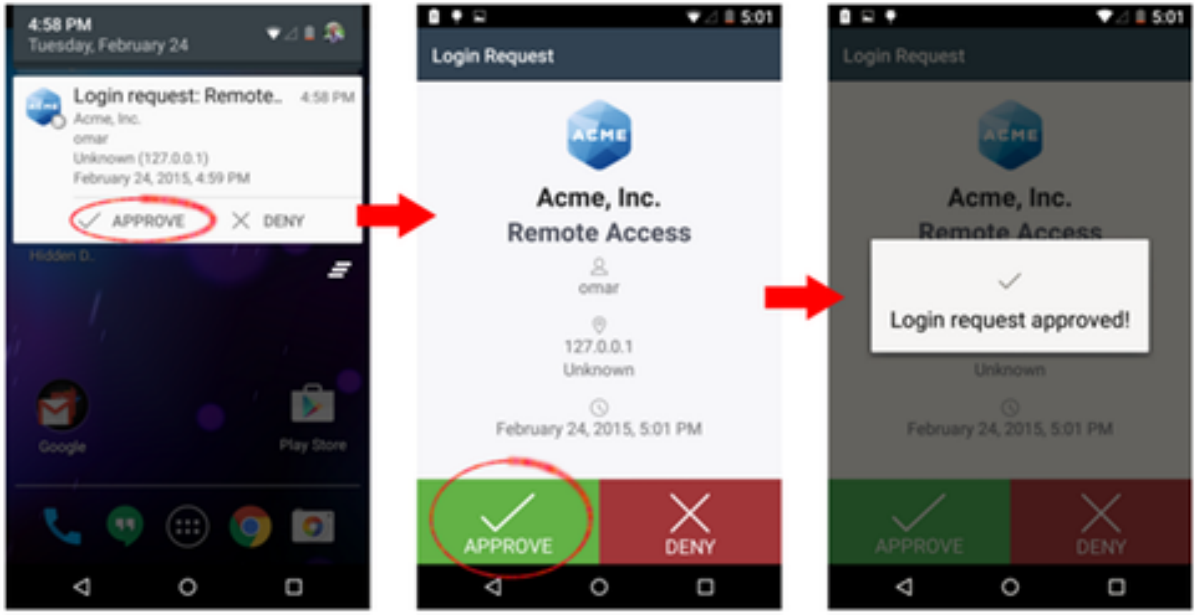
01 Getting Started

Login

1. Open up Chrome
2. Navigate to: [MedicineBow OnDemand]
3. Type in your provided username and password. Usually this will be your UWYO username and password, unless you are using an assigned training account.
4. Authenticate using your preferred 2 factor method (expandable directions below):

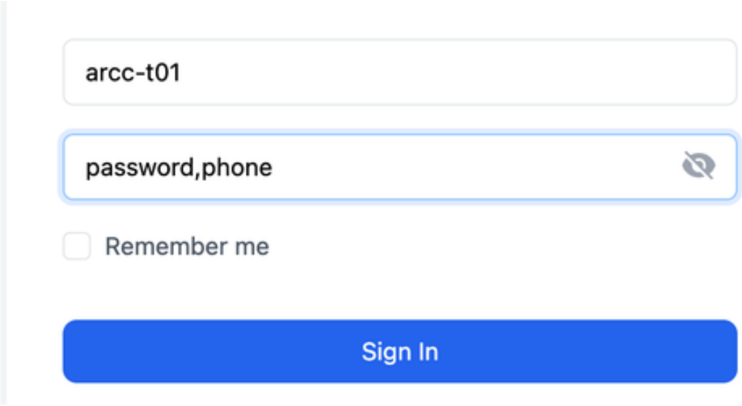
⌄ Duo Mobile push:

If you usually get a two-factor push to your phone, just hit enter after entering your username and password, then complete authentication by approving the push on your device.



⌄ Phone Call:

Without hitting enter after typing in your username and password, in the password text box, append a comma (,) to the end of your password, then append phone as shown in the screenshot below:



arcc-t01

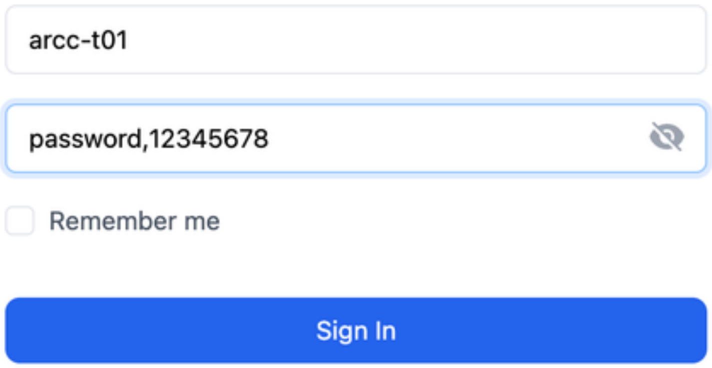
password,phone

□ Remember me

You should get a phone call on your main phone # associated with your two factor account. Answer this call and hit # to approve access.

Duo Passcode

If you prefer to use a 2 factor passcode from your Duo Mobile app, without hitting enter after typing in your username and password, in the password text box, append a comma (,) to the end of your password, then append the multi digit passcode found in duo mobile as shown in the screenshot below:

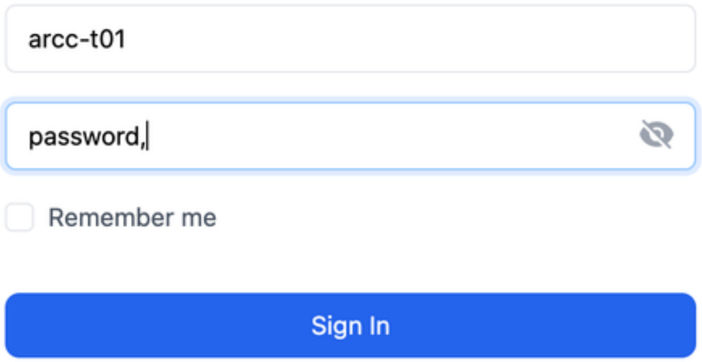


arcc-t01

password,12345678

Yubikey:

Type in the account password, then, without hitting enter, append a comma (,) to the end of the password, then touch the light on the yubikey as shown in the screenshot and photo below:

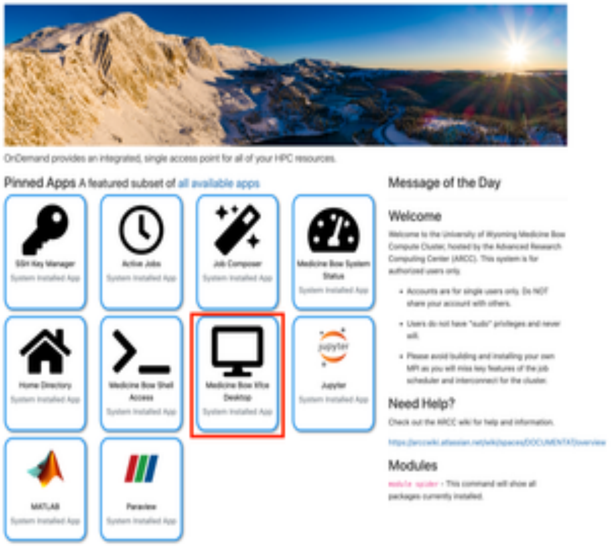


arcc-t01

password,

Then hit the green light on your yubikey to authenticate:

Start *MedicineBow Shell Access*



OnDemand provides an integrated, single access point for all of your HPC resources.

Pinned Apps A featured subset of all available apps

Message of the Day

Welcome

Welcome to the University of Wyoming Medicine Bow Compute Cluster, hosted by the Advanced Research Computing Center (ARCC). This system is for authorized users only.

- Accounts are for single users only. Do NOT share your account with others.
- Users do not have "sudo" privileges and never will.
- Please avoid building and installing your own MPI as you will miss key features of the job scheduler and interconnect for the cluster.

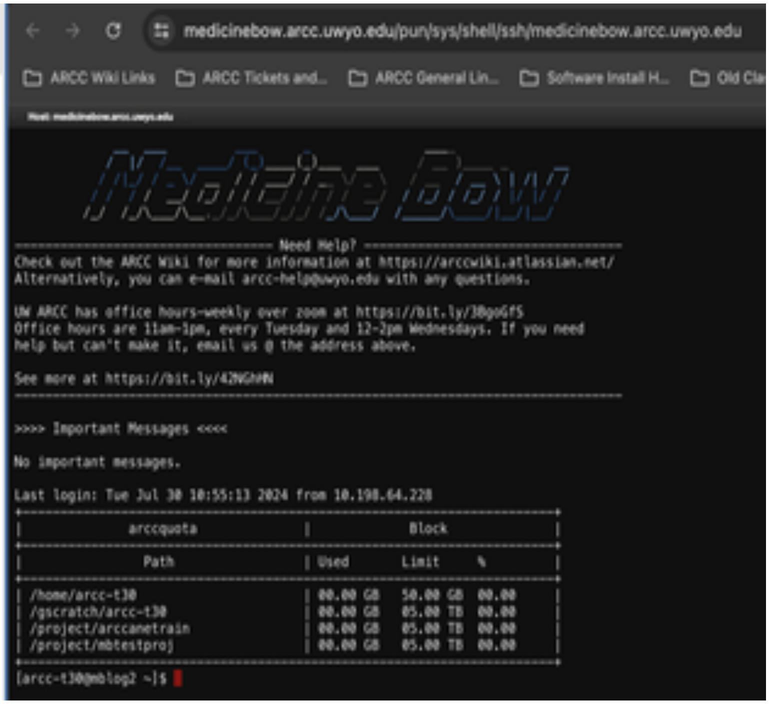
Need Help?

Check out the ARCC wiki for help and information.

https://arccwiki.atlassian.net/wiki/spaces/DOCUMENTAT/overview

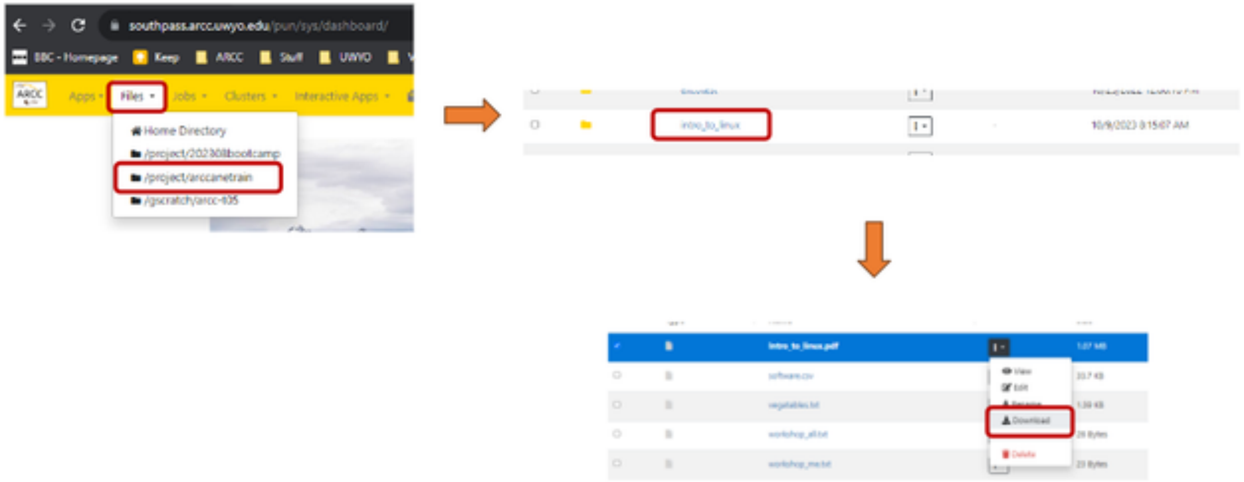
Modules

module spider - This command will show all packages currently installed.


medicinebow.arcc.uwyo.edu/pun/sys/shell/ssh/medicinebow.arcc.uwyo.edu
ARCC Wiki Links
ARCC Tickets and...
ARCC General Lin...
Software Install H...
Old Cla
Host: medicinebow.arcc.uwyo.edu
Medicine Bow

```
---------------------------------------- Need Help? ----------------------------------------
Check out the ARCC Wiki for more information at https://arccwiki.atlassian.net/
Alternatively, you can e-mail arcc-help@uwyo.edu with any questions.

UW ARCC has office hours-weekly over zoom at https://bit.ly/3BgoGfS
Office hours are 11am-1pm, every Tuesday and 12-2pm Wednesdays. If you need
help but can't make it, email us @ the address above.

See more at https://bit.ly/42NGhHN
--------------------------------------------------------------------------------------------

>>>> Important Messages <<<<

No important messages.

Last login: Tue Jul 30 10:55:13 2024 from 10.198.64.228
+----------------------------------------------------------------------------+
|              arccquota              |               Block                  |
+----------------------------------------------------------------------------+
|                Path                 | Used        Limit      %             |
+----------------------------------------------------------------------------+
| /home/arcc-t30                      | 00.00 GB   50.00 GB   00.00          |
| /gscratch/arcc-t30                  | 00.00 GB   05.00 TB   00.00          |
| /project/arccanetrain               | 00.00 GB   05.00 TB   00.00          |
| /project/mbtestproj                 | 00.00 GB   05.00 TB   00.00          |
+----------------------------------------------------------------------------+
[arcc-t30@mblog2 ~]$ 
```

Download Slides



SSH

Goal: Provide new HPC users with common steps to log into a cluster using SSH on Beartooth as an example.

- What is SSH?
- SSH Clients
- Ex: SSH to Beartooth with ARCC Training Account
- Ex: SSH enabling X11

What is SSH?

SSH stands for The Secure Shell Protocol. This is a network protocol for operating network services securely over an unsecured network. Typically users use ssh for remote access to HPC systems and ARCC users may use ssh to connect to our HPC resources. SSH allows one to login to a remote system, then remotely execute commands on the system, but virtually any network service can be secured with ssh.

SSH Clients

Your ssh client may be different than your neighbors. SSH clients differ between devices, OS versions, and end user preferences but they all use the same underlying protocol (SSH) to connect to remote servers.
Default Clients for common OS's are shown below:

OS Versions	Ubuntu (Debian) Linux OS	Mac OS	Windows OS
Default SSH Client	OpenSSH	Terminal	OpenSSH
Popular User Installed SSH Clients	PuTTY, MobaXterm, Termius	Termius, iTerm2, CyberDuck	MobaXterm, Powershell, PuTTY

Ex: SSH to Beartooth with ARCC Training Account

You have an Existing Account: Log on

- Open up a terminal.
- Use a client such as MobiXTerm

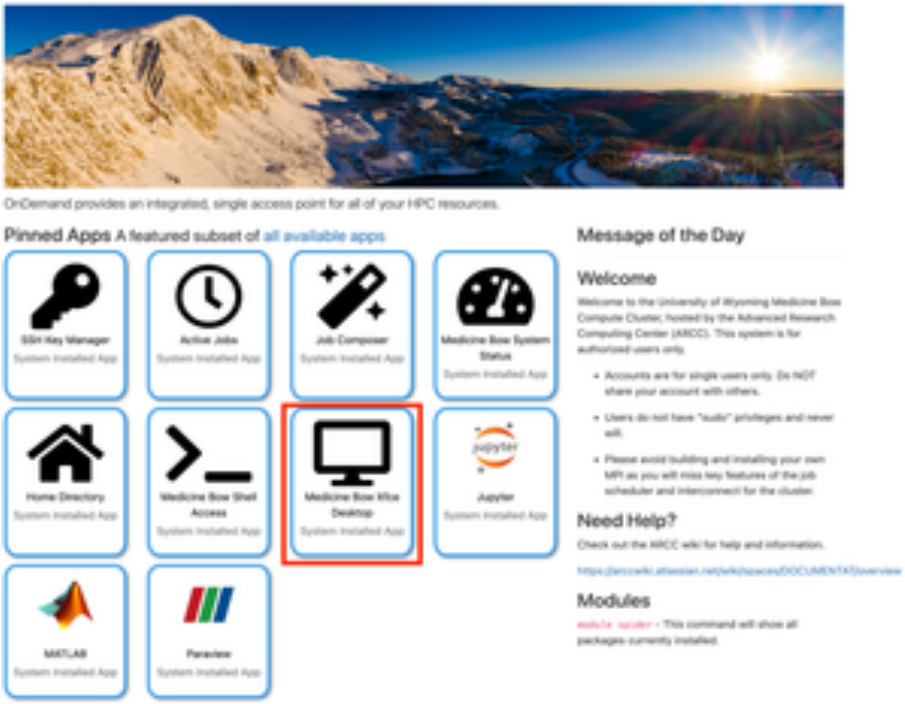
An ssh command in Command Line Interface is broken down into `username`, '@' symbol, and `servername`. As an example:

```
ssh arcc-t01@medicinebow.arcc.uwyo.edu
[arcc-t01@mblog1 ~]$
# UW: MedicineBow (mblog1/mblog2)
```

In the above ssh example, we want to use `ssh` to connect with username `arcc-t01` to servername `beartooth.arcc.uwyo.edu`

Temporarily use a test account:

1. Open up Chrome
2. Navigate to: [MedicineBow On Demand]()



OnDemand provides an integrated, single access point for all of your HPC resources.

Pinned Apps A featured subset of all available apps

Message of the Day

Welcome

Welcome to the University of Wyoming Medicine Bow Compute Cluster, hosted by the Advanced Research Computing Center (ARCC). This system is for authorized users only.

- Accounts are for single users only. Do NOT share your account with others.
- Users do not have "sudo" privileges and never will.
- Please avoid building and installing your own MPI as you will miss key features of the job scheduler and interconnect for the cluster.

Need Help?

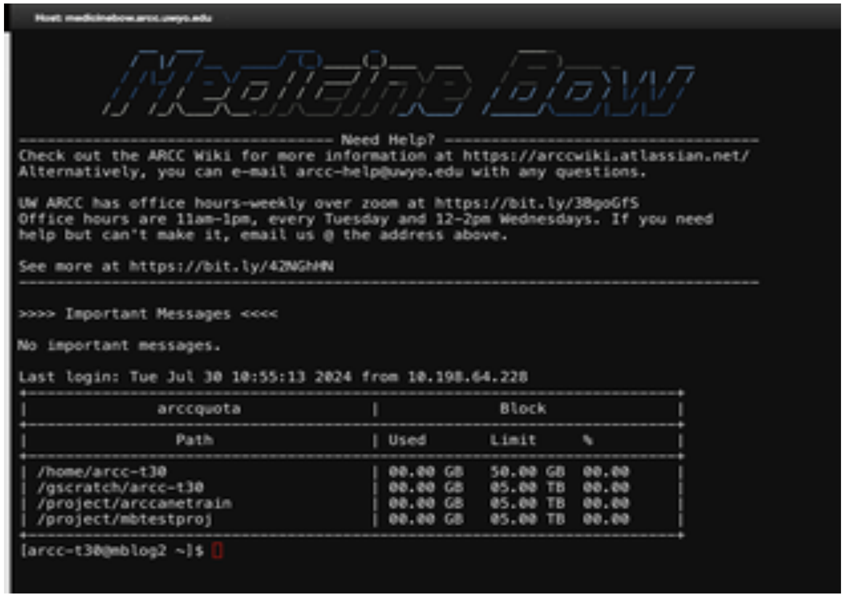
Check out the ARCC wiki for help and information.

https://arccwiki.atlassian.net/wiki/spaces/DOCUMENTAT/overview

Modules

`module spider` - This command will show all packages currently installed.

3. Start *MedicineBow Shell Access*



```
------------------------------------- Need Help? ---------------------------------------
Check out the ARCC Wiki for more information at https://arccwiki.atlassian.net/
Alternatively, you can e-mail arcc-help@uwyo.edu with any questions.

UW ARCC has office hours-weekly over zoom at https://bit.ly/38goGfS
Office hours are 11am-1pm, every Tuesday and 12-2pm Wednesdays. If you need
help but can't make it, email us @ the address above.

See more at https://bit.ly/42NGhHN
----------------------------------------------------------------------------------------

>>>> Important Messages <<<<

No important messages.

Last login: Tue Jul 30 10:55:13 2024 from 10.198.64.228
+-----------------------------------------------------------------------------+
|                 arccquota                 |               Block             |
+-----------------------------------------------------------------------------+
|                   Path                    | Used        Limit      %        |
+-----------------------------------------------------------------------------+
| /home/arcc-t30                            | 00.00 GB    50.00 GB   00.00    |
| /gscratch/arcc-t30                        | 00.00 GB    05.00 TB   00.00    |
| /project/arccanetrain                     | 00.00 GB    05.00 TB   00.00    |
| /project/mbtestproj                       | 00.00 GB    05.00 TB   00.00    |
+-----------------------------------------------------------------------------+
[arcc-t30@mblog2 ~]$
```

Ex: SSH enabling X11

Previously, we stated that additional network services can be secured with SSH. In the following example, we will connect using ssh to beartooth and enable X11 forwarding, which is a service allowing for graphics.

To use graphical applications on the remote system you will need to enable X11 forwarding. To do this with ssh you can look up in the manual to see what flag you need to add by typing `man ssh`.

Looking at the options we can find we can use a capital 'X' flag `-X` to enable X11 forwarding and a capital 'Y' flag `-Y` for secure X11 forwarding. Which one to use is up to you, but in most cases `-X` will be sufficient. If you are on a mac, you will need to use -Y. See the example below:

```
ssh -X arcc-t01@medicinebow.arcc.uwyo.edu
```

SSH Keys for Authentication

Goals:

1. Provide users with information on what an SSH Key is, how it works, and the benefits of using one.
2. Explain recommended best practices for SSH key security.
3. Walk new users through an example setting up SSH keys to authenticate to ARCC HPC clusters.
4. Guide users to the locations of step-by-step instructions for configuring an SSH key specific to their device, OS, and client application.

What are SSH Keys?

Every HPC user at ARCC has an option for private identity keys on each system they have access to. These are private keys associated with that user’s identity on an ARCC HPC cluster. On our systems, the user also has a certificate associated with their private identity key.

On newer ARCC HPC systems, users may create a new SSH key by logging into the OnDemand resource associated with the HPC, and creating a key using the SSH key Manager application.

Warning: Please be careful with these files. **Do not change their permissions, put them in an insecure digital location, or share them with others**. They are your “virtual keys” to log in as yourself on the HPC. If provided to or shared with others, they will be able to log into that ARCC HPC resource **as you**

Benefits of using an SSH Key for HPC Authentication

- **Improved Security**
  - When using private keys to authenticate, users do not need to transmit their username and password information over the network. Because private keys are kept on your local machine, they are less vulnerable to interception and attack.
  - Remote systems configured to only accept SSH Key Authentication are more secure than authenticating with a username and password alone. Secure environments should require authentication using “something you know, something you have, something you are”. Ideally, when encrypted with a passphrase, an SSH key covers 2 of those 3 with the passphrase covering something you know, and the private key covering something you have. On some devices, you may have the option to replace a passphrase with “something you are” such as a fingerprint or other biometric scanner to decrypt your key files.
- **Improved Access Control**
  - SSH keys control access to HPC resources by restricting access only to authorized users with corresponding private keys. Each user is provided a unique key associated with their identity and permissions on the system.
  - This makes it easier to revoke compromised users without requiring password changes, while still allowing all other existing users to authenticate normally.
- **Convenience**
  - Once configured appropriately, SSH keys are often more convenient and increase user productivity. For security, and appropriate configuration, we recommend always encrypting keys with a unique passphrase.
  - Tools like an ssh-agent can hold keys in memory allowing access to the ssh client which saves users from needing to enter their key passphrase repeatedly and reducing the likelihood of failed authentication when repeatedly entering passwords.
- **Automation**
  - SSH keys may be used in scripts and automation tools to automate tasks that would require logging into the remote server or HPC. This can make activities on the HPC easier and reduces the risks associated with password exposure.

SSH Key Management and Security

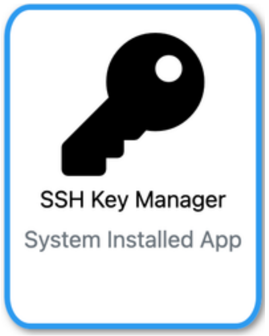
When you set up your SSH key your device, please follow best practices:

- Don’t share your SSH key with others
- Encrypt your private key files with a passphrase
- Set up SSH keys with appropriate permissions
- Do not set up SSH keys on shared devices
- If a device storing your SSH keys becomes compromised, use a different, uncompromised device to log into OnDemand. Go to the SSH Key Manager application to revoke your old key and create a new one. If you need assistance, please contact arcc-help@uwyo.edu immediately.

Creating a new key

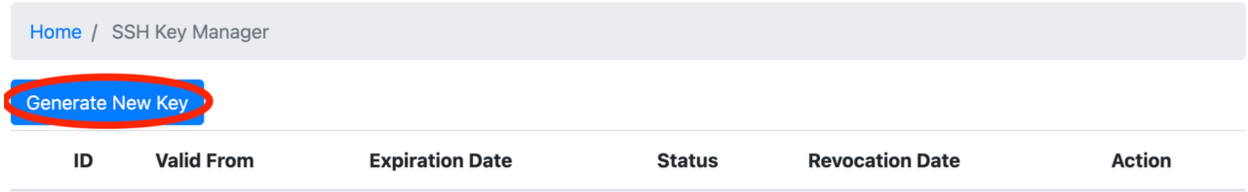
To set up access:

1. First, log into the OnDemand resource for the HPC you want to set up SSH keys for.
    1. **For MedicineBow**, log in at https://medicinebow.arcc.uwyo.edu/. Step-by-step directions for logging into MedicineBow OnDemand are available here.
    2. **For WildIris**, log in at https://https://wiodm01.arcc.uwyo.edu/. Step-by-step directions for logging into WildIris OnDemand are available here.
2. Once you’re logged in, you should be presented with the HPC Dashboard. Click the following icon to set up SSH key authentication:



3. Each key is associated with your **identity**, therefore you do not need to create a new key for every client you use to ssh into the HPC.

   If you haven't set up an SSH key previously, you should see an empty screen/list with the option to generate a new a key. Click that button if you need to set up a key.

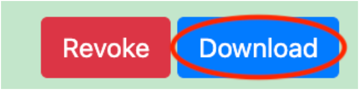


ID	Valid From	Expiration Date	Status	Revocation Date	Action

   Doing this will create a new set of files associated with your login to the HPC.

   If you've already created a key previously you don't need another one. Skip this step and download a key you've already generated for your account as described in the next step.

4. Click the download button associated with the key ID for your ssh key to download them to your client/computer.



Please be careful with these files. **Do not change their permissions, put them in an insecure digital location, or share them with others**. They are your “virtual keys” to log in as yourself on the HPC. If provided to or shared with others, they will be able to log into that ARCC HPC resource **as you**

Client Configuration

After creating and downloading your Personal SSH Identity Keys, the keys must now be set up on the system from which you’re going to be logging into the cluster from. As mentioned in the previous section, SSH key access should be limited only to the individual user being granted SSH access.

Client configuration is dependent on the device and OS from which you’ll be accessing the HPC using SSH.

Windows specific instructions are available here

Mac specific instructions are available here

Linux specific instructions are available here

Revoking and Replacing SSH Keys

Goals:

1. To provide users with information on best security practices for SSH keys
2. Provide step by step instructions for users to manage their SSH keys in the HPC Key Management Application.
    1. This includes Revocation, regenerating, and reconfigure keys on different devices.

When to revoke and regenerate your SSH keys

At some point, it may be necessary to revoke your old SSH key and create a new one. Situations that may require revoking your old ssh keys and creating new keys include:

1. Device compromise:
    1. A device upon which you store your ssh key files has been compromised, due to malware, malicious actors gaining access to log in as you on your device, or malicious actors gaining access to data stored on your device.
2. Data compromise:

    1. Your key files were copied or accessed by someone other than yourself
    2. You backed up your key files to a location outside your device that was subject to a compromise
3. Following good security practices:

    1. It is recommended that ssh keys be rotated as part of a remediation process to ensure any keys that may have been compromised since their initial generation cease to be usable. ARCC recommends rotating your keys every 6 months (similar to requiring password changes at regular intervals).

Using SSH Key Manager to revoke and regenerate SSH keys

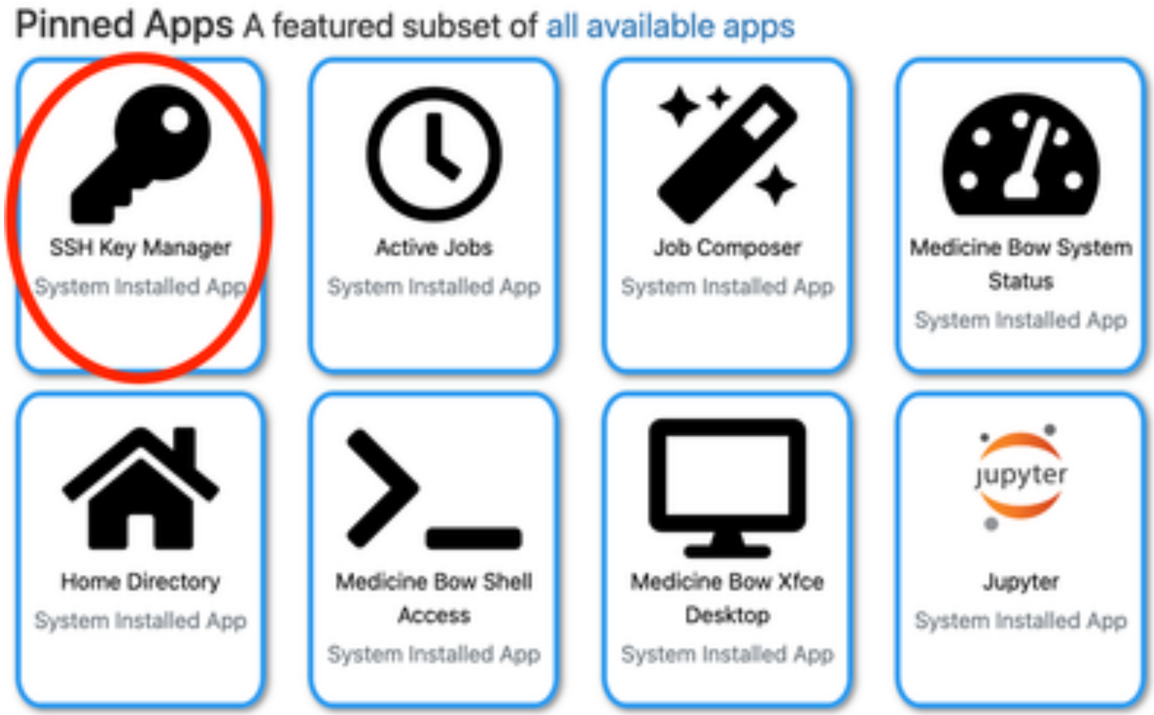
Note: if you are revoking and regenerating your ssh keys due to a compromise, you must perform the following steps on a different, uncompromised device

1. Open a new browser window and go to the OnDemand URL (3rd column in table below) for the HPC in which you'd like to revoke and regenerate your keys
2. Log in per directions on the linked wiki page (right-most column) associated with the HPC cluster in which you would like to regenerate keys

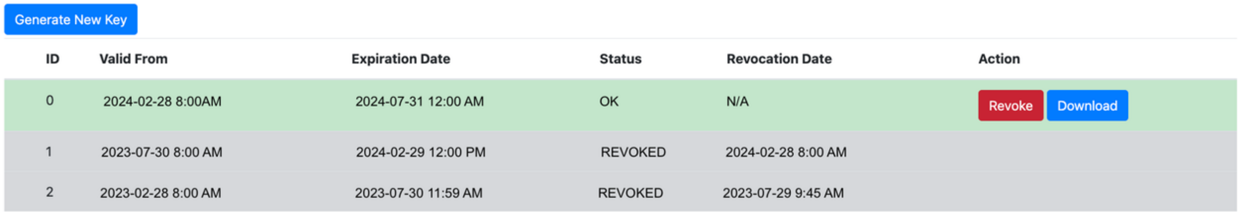
To facilitate greater access and usability of our HPC services, UW ARCC has configured OnDemand for 3 of our HPC clusters:

HPC Cluster	OnDemand Name	OnDemand URL	ARCC Wiki Pages for HPC-specific OnDemand Services
MedicineBow	MedBow OnDemand	https://medicinebow.arcc.uwyo.edu	Web Access to MedicineBow: OnDemand
Beartooth	Southpass	https://southpass.arcc.uwyo.edu	Web Access to Beartooth: Southpass
WildIris	WildIris ODM	https://wiodm01.arcc.uwyo.edu	Web Access to Wildiris: OnDemand

3. Once logged in, click on the SSH Key Manager application in the dashboard to manage your keys.

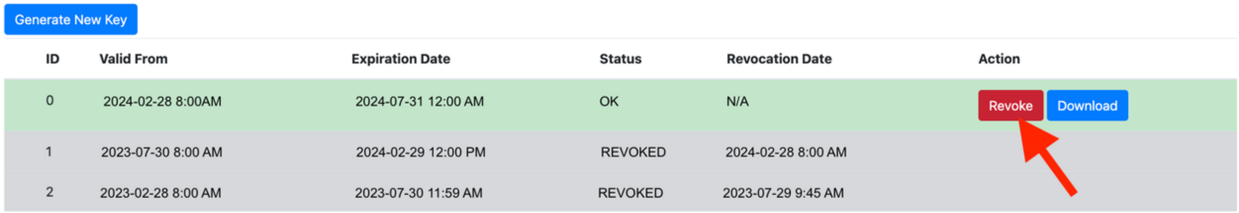


4. This will bring up the key management screen. At the bottom is a list of any keys you've created previously. If you have revoked keys in the past, you will have a list of your prior keys (in gray) and your current key (in green). Otherwise you will have only your current authentication key (highlighted in green)



ID	Valid From	Expiration Date	Status	Revocation Date	Action
0	2024-02-28 8:00AM	2024-07-31 12:00 AM	OK	N/A	Revoke Download
1	2023-07-30 8:00 AM	2024-02-29 12:00 PM	REVOKED	2024-02-28 8:00 AM	
2	2023-02-28 8:00 AM	2023-07-30 11:59 AM	REVOKED	2023-07-29 9:45 AM	

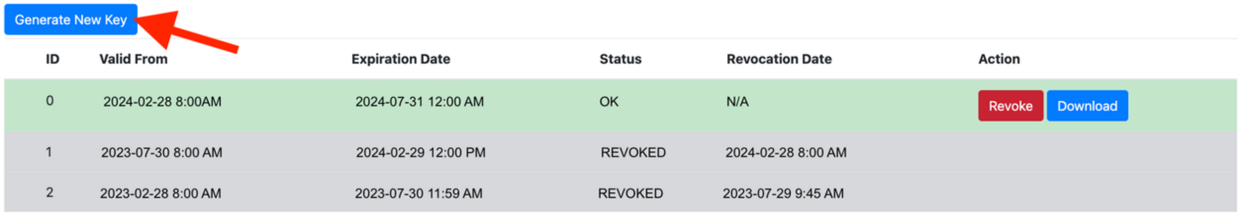
5. Click the red "Revoke" button associated with your current key (highlighted in green).



ID	Valid From	Expiration Date	Status	Revocation Date	Action
0	2024-02-28 8:00AM	2024-07-31 12:00 AM	OK	N/A	Revoke Download
1	2023-07-30 8:00 AM	2024-02-29 12:00 PM	REVOKED	2024-02-28 8:00 AM	
2	2023-02-28 8:00 AM	2023-07-30 11:59 AM	REVOKED	2023-07-29 9:45 AM	

Your latest key will now turn from green to gray and should change status to “REVOKED”.

6. Click the Generate New Key button

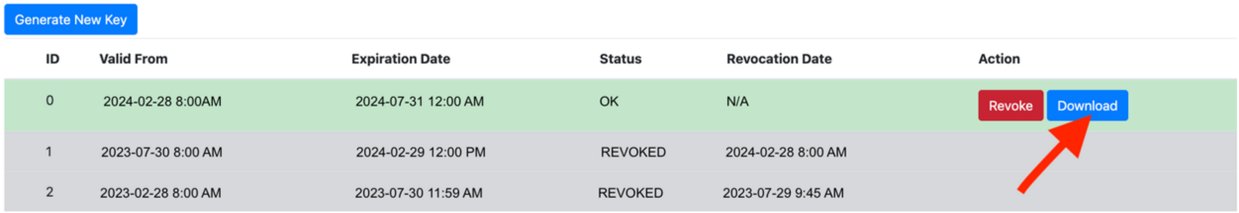


ID	Valid From	Expiration Date	Status	Revocation Date	Action
0	2024-02-28 8:00AM	2024-07-31 12:00 AM	OK	N/A	Revoke Download
1	2023-07-30 8:00 AM	2024-02-29 12:00 PM	REVOKED	2024-02-28 8:00 AM	
2	2023-02-28 8:00 AM	2023-07-30 11:59 AM	REVOKED	2023-07-29 9:45 AM	

You may receive a message asking if you’re sure you want to do this. Click Continue.

7. A new key will be created, highlighted in green. This is your current SSH key set to authenticate into the HPC resource.

Click the download button. This will download your new key files to the local device from you’re currently accessing OnDemand.



ID	Valid From	Expiration Date	Status	Revocation Date	Action
0	2024-02-28 8:00AM	2024-07-31 12:00 AM	OK	N/A	Revoke Download
1	2023-07-30 8:00 AM	2024-02-29 12:00 PM	REVOKED	2024-02-28 8:00 AM	
2	2023-02-28 8:00 AM	2023-07-30 11:59 AM	REVOKED	2023-07-29 9:45 AM	

Replacing SSH Keys on your Device

Before configuring your new ssh keys on your devices (usually this is your main workstation or laptop) you must remove your old keys.
As always, ARCC recommends only setting up SSH authentication keys on devices you have sole access to, and not on shared devices. If you do set up an ssh key for authentication on a shared device, only do so on computers where individuals log into separate, individual profiles on the computer. If you're not sure how to determine this, contact arcc-help@uwyo.edu

Expand the section associated with your specific device OS and follow directions to remove your old SSH keys before replacing them with your new keys.

On a Windows PC

Removing SSH Keys on a Windows PC

The standard location for ssh key files on a windows system are in your personal User directory in a hidden subfolder named `.ssh`. On a normal windows PC, this would be under `C:\Users\<your_username>\.ssh\`. If you have configured your keys using a non-standard key location, it is your responsibility to be aware of this location.

1. Open file explorer (By hitting your windows key + E, or clicking the file explorer icon from your start menu or taskbar)
2. Browse to the directory in which your key files are stored
3. Delete the following files:
    1. id_ecdsa
    2. id_ecdsa.pub
    3. id_edcsa-cert

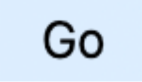
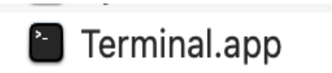
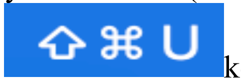
Note: we have found that Microsoft sometimes categorizes file types incorrectly. The public key and cert files may be categorized incorrectly as a Microsoft Publisher file and icon. This is ok.

4. Once your old key files have been deleted, you may configure your new keys. Follow the remaining directions [here](#) to configure your new keys on your Windows PC

On a Mac

Removing SSH Keys on a Mac

The standard location for ssh key files on a Mac OS computer are in your personal `/home` directory in a hidden subfolder named `.ssh`. On most Macs, this would be under `/Users/<your_name_on_mac>/.ssh/`. If you have configured your keys using a non-standard key location, it is your responsibility to be aware of this location.

1. Open your terminal (→  → →  or hit  keys)
2. If your SSH keys are stored in the standard location, change directories to your .ssh directory for your user account on the Mac with the following command: `cd ~/.ssh` otherwise cd to the directory in which your keys are stored.
3. Remove your old keys using the rm command: `rm id_ecdsa id_ecdsa-cert.pub id_ecdsa.pub`
4. Once your old key files have been deleted, you copy over and configure your new keys as described in the linked instructions [here.](#)

On a Linux PC

Removing SSH Keys on a Linux Computer

The standard location for ssh key files on a Linux OS computer are in your personal `/home` directory in a hidden subfolder named `.ssh`. On most Linux machines, this would be under `/home/<your_username>/.ssh/`. If you have configured your keys using a non-standard key location, it is your responsibility to be aware of this location.

1. Open your choice of command line interface (shell, terminal, console, prompt, etc)

2. If your SSH keys are stored in the standard location, change directories to your .ssh directory for your home on the PC with the following command: `cd ~/.ssh` otherwise cd to the directory in which your keys are stored.
3. Remove your old keys using the rm command: `rm id_ecdsa id_ecdsa-cert.pub id_ecdsa.pub`
4. Once your old key files have been deleted, you copy over and configure your new keys as described in the linked instructions here.

Tour of an ARCC HPC

Goals: Walk through accessing an ARCC HPC and navigating directories

If users have attended previous workshops, this will be review.

Opening Screen:

- Shows message of the day
- Lists storage usage - across project spaces
  - You can see this again by calling: arccquota
  - Also shows directories specific to arcc HPCs

```
General Format:[<username>@<server/node-name> <folder>]$
[arcc-t30@mblog2 ~]$ arccquota
+----------------------------------------------------------------------+
|              arccquota              |             Block              |
+----------------------------------------------------------------------+
|                Path                 | Used       Limit     %         |
+----------------------------------------------------------------------+
| /home/arcc-t30                      | 00.00 GB   50.00 GB  00.00     |
| /gscratch/arcc-t30                  | 00.00 GB   05.00 TB  00.00     |
| /project/arccanetrain               | 00.00 GB   05.00 TB  00.00     |
|                                                                      |
+------------------------------------------------------------------------+
[arcc-t30@mblog1 ~]$
```

ARCC HPC: FileSystem

Type	Location	Description	Notes
home	/home/<username>	Personal storage space associated with user's account. For configuration files and smaller software installations.	Smaller allocation
project	/project/<project-name>/	Space to collaborate among project members. Data here is persistent and is exempt from purge policy.	All project members have read/write at this level.
project-user	/project/<project-name>/[username]	Storage specific to username within project space. Project members can read but only you may write.	
project-software	/project/<project-name>/software	Storage space to install software to be shared among project group members.	Only on MedicineBow
gscratch	/gscratch/<username>	Scratch space to perform computing for individual users.	Data here is subject to a purge policy.
node local scratch	/lscratch	Only on compute.	
memory filesystem	/dev/shm	RAM-based tmpfs available as part of RAM for very rapid I/O operations; small capacity.	

See here for information about directory quotas

Home, Project, and Gscratch Folders:

```
# Home folder:
[]$ cd ~
[]$ pwd
/home/arcc-t05
```

```
[]$ cd /gscratch/arcc-t05
# Shared project space
[]$ cd /project/arccanetrain/
[arcc-t05@blog1 arccanetrain]$ ls
arcc-t01  arcc-t06  arcc-t11  arcc-t16  arcc-t21  arcc-t26  brewer       salexan5
arcc-t02  arcc-t07  arcc-t12  arcc-t17  arcc-t22  arcc-t27  excotest
arcc-t03  arcc-t08  arcc-t13  arcc-t18  arcc-t23  arcc-t28  intro_to_hpc
arcc-t04  arcc-t09  arcc-t14  arcc-t19  arcc-t24  arcc-t29  lreilly
arcc-t05  arcc-t10  arcc-t15  arcc-t20  arcc-t25  arcc-t30  mkillean
```

Copy files:

```
[]$ cd
[~]$ cp -r /project/arccanetrain/intro_to_hpc/ .
[~]$ cd intro_to_hpc/
[intro_to_hpc]$ ls
Intro_to_hpc.pdf  python01.py  python01.py.fixed  run_gpu.sh  run.sh
```

Next Steps

Previous	Workshop Home
Revoking & Replacing SSH Keys	Intro to Accessing the Cluster

Use the following link to provide feedback on this training: https://forms.gle/qQ8b7SxGJbo2U6y98 or use the QR code below.