SAS Computing Environment User’s Guide

July 2018, Version 6

Defense Health Agency

**Revision History**

|  |  |  |
| --- | --- | --- |
| **Version** | **Date** | **Description of Changes** |
| 5.6 | October 2010 | * Clarified use of Export Transmittal request in regards to PHI data * Updated Section B-6: REF Data Types |
| 5.7 | April 2011 | * Clarified new user password instructions on pg. 26 * Added statement on maximum number of programs submitted on pg 34 * Added information on CAPER Enhanced on pg 75 * Updated metadata access instructions in Section A-9 * Updated DD2875 instructions for including metadata access for new account requests * Included password server OOB and Non-OOB (\*.mil only) IP addresses in sections A-3 and A12 |
| 5.8 | July 2011 | * Updated Section A-5 for submitting a SAS program * Changed MDR Functional Proponent for sending PHI download/upload notifications (p 16) * Updated MDR application and instructions * Changed BEA reference to DHCAPE |
| 5.9 | February 2012 | * Updated Export Transmittal form (Attachment A-2) * Updated MDR AARF |
| 5.10 | July 2016 | * Updated contact information * Updated first time login instructions for OOB, PuTTY and WinSCP * Updated 2875 instructions * Removed old forms and references to previous systems and processes * Removed HSM mechanical detail section, Load Leveler detail section, and complete list of tables and update times. Added references to the MDR data dictionary * 2875, AARF, and other forms removed. Links to online locations added. |
| 6.0 | July 2018 | * Major changes to update after transition to Capacity Services |

**CTRL + Click to go to the locations in the Table of Contents below:**

Contents

[I. Introduction and MDR Overview 3](#_Toc520377104)

[II. System Overview and Technical Architecture 5](#_Toc520377105)

[Data Refresh and Availability 5](#_Toc520377106)

[Operational Policies/Constraints 6](#_Toc520377107)

[System Training 6](#_Toc520377108)

[Configuration Management (CM), Backup, and Environment 6](#_Toc520377109)

[Backup of Output Products 6](#_Toc520377110)

[III. Space Allocation and Related Issues 6](#_Toc520377111)

[IV. Storing and Securing Privacy Act and HIPAA Data 7](#_Toc520377112)

[Keeping Logs 7](#_Toc520377113)

[V. Getting Started 8](#_Toc520377114)

[Requesting SCE Access 8](#_Toc520377115)

[Instructions for filling out DD2875 Form 9](#_Toc520377116)

[Connecting to the SCE 11](#_Toc520377117)

[Secure Shell (SSH) Login 18](#_Toc520377118)

[Transferring Files to/from the SCE 21](#_Toc520377119)

[Submitting SAS Jobs in the SCE 23](#_Toc520377120)

[Moving Files to the SCE from External Systems 25](#_Toc520377121)

[Copying Files from the SCE to External Media 28](#_Toc520377122)

[Changing Your Password 29](#_Toc520377123)

[UNIX File Naming Conventions 35](#_Toc520377124)

[The UNIX Directory Tree 36](#_Toc520377125)

[Getting Around Directories 36](#_Toc520377126)

[Appendix A: The PICO Editor (For editing in UNIX) and VI editor 37](#_Toc520377127)

[Basic VI Editor 40](#_Toc520377128)

# Introduction and MDR Overview

The SAS Computing Environment (SCE) provides authorized individuals with access and query capability to specified Military Health System (MHS) Data Repository (MDR) data sets. The SCE is an extension of the existing Solution Delivery Division (SDD) architecture and does not add additional data elements, file types, or functionality beyond that offered by the existing SDD product suite. This User Guide addresses the processes for accessing and utilizing the SCE.

Data sets contained within the MDR include workload, cost, population, enrollment, demographic, and reference data for the MHS. The data sets are arrayed in a structured manner. They are available post processing and are represented as a subset of the MDR file catalogue:

* According to a defined periodicity or update cycle;
* Processed using known, tested software - with identified business rules;
* Quality controlled, documented, and reviewed; and
* Released for specified use.

**MDR Data Sets**

Below is some general content commonly used by users. To see all available MDR tables, file locations, refresh time periods, data fields and data field types use the current MDR Data Dictionary located at <http://health.mil/Military-Health-Topics/Technology/Support-Areas/MDR-M2-ICD-Functional-References-and-Specification-Documents>.

**General Content:**

**MTF Clinical System Data**

* Direct Care Encounter Data (*Comprehensive Ambulatory/Provider Encounter Record, CAPER*), Basic and Enhanced
* Direct Care Inpatient Data (*Standard Inpatient Data Record, SIDR*)
* Appointment Data (*APPT*)
* Ancillary (ANCIL) Laboratory and Radiology
* Referral Data
* Case Management

**Manpower, Workload, Expense Data**

* Expense Assignment System (*EAS-IV*)

**Beneficiary Demographics Data**

* DEERS Beneficiary Level
* DEERS Enrollment
* DEERS Longitudinal Enrollment

**Centralized Pharmacy Data**

* Pharmacy Data Transaction Service (*PDTS*)

**Purchased Care Data**

* TRICARE Encounter Data – Institutional Data (*TEDI*)
* TRICARE Encounter Data – Non-institutional Data (*TEDNI*)
* TRICARE Encounter Data – Provider Data (*TEDPR*)

**Centralized MHS System Management Data and Reference Tables**

* Geographic Data (*OmniCAD*)
* Entity Identifiers/Relationships (*DMISID Index*)
* Provider Specialty Codes

**Dental Data**

* Active Duty Dental Plan (ADDP)
* Tricare Dental Plan (TDP)

**Death Data**

* Casualty Data
* Master Death File Data
* Encounter Death Data

**Designated Provider Data (Desprov)**

* Clinical Data
* Pharmacy Data
* Provider Data

**Users**

The SCE presumes the enterprise-level power users possess a thorough knowledge of SAS and existing MHS data sets and are experienced healthcare analysts.

# System Overview and Technical Architecture

The data in this environment is a combination of SAS datasets and ASCII flat files. Most processed data reside in SAS data set form and take advantage of SAS procedure and library functions. The environment has no user interface in the traditional sense. It is intended for expert analysts only.

**Software**

The SCE provides access to authorized users via secure communication technologies (i.e. SSH – See Section VII, *Overview of Access Requirements*). Users do **not** have access to Graphical User Interface (GUI) functionality provided by the Common Desktop Environment (CDE). Some of the tools supported by the SCE are identified in Table 1.

**Table 1. Corporate and Service Node Support Tools**

|  |  |  |
| --- | --- | --- |
| **SAS v9.3** | **Text Editors** | **Other** |
| Base SAS SAS EG | PICO  vi | PuTTY WinSCP |

**Storage - Online**

Online disk storage is available to the SCE. Section X, entitled *Space Allocation and Related Issues*, contains additional information on SCE online disk storage requirements.

**Storage – Near-line**

In addition to online disk storage, the SCE offers near-line resources to some users. Near-line resources consist of tape subsystems that allow users to conserve online disk space while retaining the ability to store and retrieve data. Additional information on near-line storage can be found in Section X, entitled *Space Allocation and Related Issues*.

**Computing Resources Management (Job Priorities and Scheduling)**

System administrators will monitor computing resources. Additional information on how computing resources are managed to avoid contention and maximize performance can be found in Appendix C, entitled *Load Leveler and Computing Resources Management*.

## Data Refresh and Availability

The MDR data sets in this environment will be refreshed with current week, month, quarter, or yearly data immediately after MDR processing is completed. For MDR data sets that are processed, the update will be loaded upon receipt and completion of Quality Control (QC). For more information on data sets you can consult the MDR data dictionary located at <http://health.mil/Military-Health-Topics/Technology/Support-Areas/MDR-M2-ICD-Functional-References-and-Specification-Documents>

## Operational Policies/Constraints

Operational policies and constraints are outlined below:

* Support: System and database administration, firewall administration, and data and systems configuration control are provided by SDD system administration staff.
* Configuration Management (CM): Reports and “result sets” generated by users will not be placed under CM control.
* Access Restrictions: System level access will be restricted to SDD system administration staff.
* System Security: This environment is considered an access point to the corporate MDR and as such will undergo security testing and be subject to all associated security documentation requirements.
* System Backup: Backup and recovery of output/work products are controlled by SDD System Administration Staff.

## System Training

The Basic User’s Guide for UNIX and SAS are available to assist users. The SDD program office does not provide training.

## Configuration Management (CM), Backup, and Environment

Hardware and Software CM will be handled in accordance with the policies and procedures of the SDD Program Office. Specifically, SDD owned software, scripts and utilities will be maintained under CM control. Scripts, programs, reports and “result sets” created by SCE users will not be managed by CM.

## Backup of Output Products

Output/work products in specifically defined user directories will be written daily to backup storage. Output/work products deleted from the SCE will be deleted from backups within thirty days. SDD system administration staff control backup and restoration of output/work products.

# Space Allocation and Related Issues

A file system is a method of storing and organizing data files, such as SAS programs, output files, SAS datasets, and text files. It also allows for manipulation and retrieval of data within and across file systems. Every file system on the SCE has rules that set permissions for user access.

As these file systems contain private rather than MDR files, the government and/or functional owner of the file system is responsible for:

* Ensuring the file system contains only data authorized by law and regulation;
* Ensuring Privacy Act and Health Insurance Portability and Accountability Act (HIPAA) laws and regulations are followed; and
* Notifying SDD of both who is empowered to provide access authorizations for that file system, and through that agent, the list of users allowed into those project or sponsor- designated files.

SDD is responsible for assuring that any user granted access into the nodes has:

* The mandatory minimum paperwork complete and on file with SDD to access the SCE and MDR data sets (ADP-II clearance, Data Sharing Agreement (DSA), Cyber Awareness Certificate (previously called IA training certificate), and Account Access Request Form);
* Been identified by name and project/file system on an authorization document from the file system functional owner or access authority;
* Permission into those file systems for which the file system authority has granted access and no others.

File systems will be determined based on sponsoring organization and project designation. Permissions for access are based on the information provided in the SCE Account Access Request Form (AARF). For example /mdr/pub is generally accessible, but /mdr/apub requires special permission.

# Storing and Securing Privacy Act and HIPAA Data

Health Insurance Portability and Accountability Act (HIPAA) requires healthcare systems to record any use or discloser of an individuals’ healthcare data.

Users are responsible for full compliance with HIPAA and the Privacy Act for data created or placed into all files systems on the SCE. SDD does not track data stored in user workspace within these file systems. Private Health Information (PHI) data created as a result of programs extracting data from the MDR datasets for download or those originating outside of the SCE and imported/uploaded/keyed into these file systems must be reported via e-mail to the SCE Functional Proponent ([james.t.huber4.civ@mail.mil](mailto:james.t.huber4.civ@mail.mil)) with the subject line HIPAA download Request.

The e-mail should be sent **before the file is downloaded or uploaded**. Multiple files can be listed in the same e-mail. The e-mail needs to include a brief description of the file, approximate size, source, and destination file system, along with your identity and organization. This information may be used to determine if an Import or Export Transmittal form is required (e.g., large amounts of data).

**Downloads of PHI data that are 10,000 rows or greater requires an Export Transmittal request. Users should not download this data themselves via WinSCP or any other FTP software.**

EXAMPLE OF DOW NLOADING EMAIL:

25-March04: Downloaded Direct Care SIDR and SADR records from /xyz/abc to hard drive; ~2,500 records total, with PHI and PII data. Delivered to OTSG Decision Support Center via secure FTP (HIPAA compliant). Data deleted from hard drive after delivery. John Doe, ABC Company (Decision Support).

EXAMPLE OF UPLOADING EMAIL:

25-March-04: Uploaded DMDC-provided file containing 2,500 activated guard/reserve records with SSNs and minimal activation information, saved into the corporate node's "ABC Company" file system. John Doe, ABC Company (Decision Support).

The requirement to log the existence, distribution, and destruction of files containing PHI data created on the Corporate or Service node applies to files created from the MDR as well as those placed there by users.

## Keeping Logs

In healthcare systems such as the SCE, SDD can identify data access or discloser to the point of knowing which SCE user extracted data from an MDR data set on a specific date. In order to fulfill the remainder of the requirement for records of access, **each SCE user must retain logs of program executions on any files containing Privacy Act data**. These logs can be the normal electronic logs produced by SAS and stored by the user on the SCE. Upon request, these logs must be made available to SDD, TMA Privacy Office, or Decision Support.

One example for automatically saving the SAS logs to a dedicated log directory includes the following SAS macro which is coded at the beginning of every SAS program:

%let dir1=%str(/*main*/*secondary*/*task*/log/);

%let pgmname=%str(*xxxpgm\_name*);

%let date=&sysdate;

%let time=&systime;

%let ext1=%str(log);

%let break=%str(-);

%let final1=&dir1&pgmname&date&break&time..&ext1;

%put &final1;

proc printto log="&final1";

run; quit;

/*main* = the main directory of your dedicated workspace

/*secondary* = secondary directory, if applicable

/*task* = specific task name

/log = log directory set up for each task

*xxx* = users initials

*pgm\_name* = program name

Before running this, make sure you have created the log directory in the file path. This is where all the logs, every time the program is run, will be stored for future reference, if necessary.

Notes:

1) create task areas for easier reference

2) use program names that make sense for the task

3) user initials allows for identification of who ran the program

**If you use the above code, you MUST use the following to submit the program:**

**/main/secondary/task/log > sas pgm\_name.sas –altlog pgm\_name.log**

The –altlog <program\_name>.log portion of the command also puts a \*.log file in the directory you submitted the program from and is where the programmer can review the results of the program. So, essentially two duplicate logs are created, one for the programmer to review, the other to be HIPAA compliant. The HIPAA compliant log never gets overwritten. The reviewer log gets overwritten every time the program is rerun.

# Getting Started

# Requesting SCE Access

The AARF and 2875 forms can be found at <http://health.mil/Military-Health-Topics/Technology/Support-Areas/MDR-M2-ICD-Functional-References-and-Specification-Documents>.

Due to the sensitive nature of data contained within the SDD COMPUTING ENVIRONMENTS, there are several requirements that must be satisfied before obtaining access to the system.

1. Must be a U.S. Citizen.
2. Must have a Common Access Card (CAC).
3. Completion of the SCE Account Authorization Request Form (AARF), which includes the following requirements:
4. If applicable, an approved Data Sharing Agreement (DSA) authorizing access to MDR data from the SCE. **Civilian personnel and active duty service members conducting research and non-MHS personnel and/or contractors working for the MHS/DoD requiring access to MDR data are required to have a current Data Sharing Agreement (DSA) through their sponsoring organization on file with the Defense Health Agency (DHA) Privacy and Civil Liberties Office. If you do not have a DSA please contact DHA Privacy and Civil Liberties Office at** [dha.ncr.health-it.mbx.dsa-mail@mail.mil](mailto:dha.ncr.health-it.mbx.dsa-mail@mail.mil).
5. Experience using SAS software.
6. Completion of a DISA Form DD2875, which includes the following requirements:
   1. Completion of Cyber Awareness Training, renewed annually. A copy of the Cyber Awareness Training Certificate must be submitted with the application.
   2. Clearance level of Tier 3, ANACI/NACLC or higher.

## Instructions for filling out DD2875 Form

The Applicant/Requestor, their Manager/Supervisor, and Security Officer have separate portions of the DISA Form DD2875 to complete. Follow the step-by-step instructions below for each responsible party. If you have questions on how to fill out the form, you may submit an unsigned version for review, before obtaining signatures, or email questions about specific fields to: [beth.pelletier@alqimi.com](mailto:beth.pelletier@alqimi.com) and [corinna.barnes@alqimi.com](mailto:corinna.barnes@alqimi.com).

For the Applicant/Requestor:

1. **TYPE OF REQUEST:** Mark INITIAL if you do not have a current MDR SCE account/User ID. Otherwise mark as a MODIFICATION and include your SCE account/User ID.
2. Include the date on the top of the form.
3. **SYSTEM NAME *(Platform or Applications)***: Type **CS AIX server account, UNIX OOB access account**
4. **LOCATION *(Physical Location of System)***: Type **DISA SATX, DISA OKC**
5. Requestor/Applicant to complete **Part I**:
   1. Complete Boxes 1-8 with the Requestors/Applications information. Contractors should put **CONT** for their job title in Box 6 **JOB TITLE AND GRADE/RANK**.
   2. Box 10 must be checked showing that you completed Cyber Awareness training and the date in Box 10 must match the date on your Cyber Awareness certificate (previously called IA Training certificate). To be current, Cyber Awareness training should be completed within the last 10 months. The date should be in the format YYYYMMDD.
      1. IA Training/Cyber Awareness Challenge can be found at <http://iase.disa.mil/eta/Pages/index.aspx>
   3. Include the date in Box 12 matching the format YYYYMMDD
   4. Complete Box 11, **USER SIGNATURE** by digitally signing with your CAC. Digitally signing will be appear as an option when you hover the curser over the box.

*NOTE: This is an electronically secured form and handwritten signatures are not accepted. Signing will lock this portion of the form so make sure all fields are correct before signing*.

1. Verify your name in Box 26.
2. Complete Box 27 **OPTIONAL INFORMATION *(Additional Information)*** with the following information, and fill in the blanks for User Name, Date of Birth, EDIPN, DSA #, and PIN (Personal Identification Number). The PIN should consist of a 4 to 6 digit number which may be used to identify you.

**1.) User Name (Last, First, Middle In.):**

**2.) Date of Birth (MM/DD/YYYY):**

**3.) EDIPN (10 digit number on the back of your CAC):**

**4.) DSA # (Required for contractors):**

**5.) PIN:**

**OOB Access to SATX/OKC with UNIX profile.**

**Server account creation on the following AIX servers:**

**Production SCE: cship-name usatix8v**

**Production MCAT: cship-name usatix8z, set rlogin=false and login=true**

**ProdTest SCE:cship-name utinip1q**

**ProdTest MCAT: cship-name utinip1s, set rlogin=false and login=true**

**Set Primary Group set to "sce"**

**\*\*\*SATX SA: Once OS accounts are created on the AIX Servers please DO NOT notify the user. Instead please notify the SDD Access Office and SDD DP Ops personnel that the ID has been created.\*\*\***

1. Email the form to your manager/supervisor to complete Part II.

For the Manager/Supervisor:

Complete Part II of the form using the following step-by-step instructions. Leave Boxes 21-25 blank. Date Box 19 before signing in Box 18 electronically with your CAC card.

1. Box 13 **JUSTIFICATION FOR ACCESS** should state the job responsibilities that require access to the MDR.
2. Box 14 **TYPE OF ACCESS AUTHORIZED**: Check **AUTHORIZED**
3. Box 15 **USER REQUIRES ACCESS TO**: Check **UNCLASSIFIED**
4. Box 16 **VERIFICATION OF NEED TO KNOW** must be checked that they need this access.
5. Box 16a **ACCESS EXPIRATION DATE** must be completed if the user is a contractor. Contractors must specify Company Name, Contract Number, Expiration Date. If this information is unable to fit in Box 16a include it in Box 13.
6. Box 17 **SUPERVISOR’S NAME**: Type your name.
7. Type the date in Box 19.
8. Complete Boxes 20 – 20b.
9. Digitally sign using your CAC in Box 18 **SUPERVISOR’S SIGNATURE**. Digitally signing will appear as an option when you hover the curser over box.

*NOTE: This is an electronically secured form and handwritten signatures are not accepted. Signing will lock this portion of the form so make sure all fields are correct before signing.*

1. Email the form to the Applicant/Requestors Security Officer to complete Part III.

For the Security Officer:

A minimum Tier 3, ANACI/NACLC or higher clearance is required to gain access to the MDR SCE. The Security Officer should complete Part III and return to the manager or user for submission.

1. Complete Boxes 28 – 30.
   1. Box 28b must be Top Secret, Secret, or NA. No other values are acceptable. Values that are not Secret or Top Secret should be entered as NA.
   2. Ensure that the information matches what is currently listed in JPAS.
2. Type the date in Box 32.
3. Digitally sign using your CAC in Box 31 **SECURITY MANAGER SIGNATURE**. Digitally signing will appear as an option when you hover the curser over box.

*NOTE: This is an electronically secured form and handwritten signatures are not accepted. Signing will lock this portion of the form so make sure all fields are correct before signing.*

1. Send the DISA Form DD2875 back to the Applicant/Requestor for submittal to DHA SDD.

## Connecting to the SCE

Most users are required to use the Out-of-Band (OOB) Secured Socket Layer (SSL) Virtual

Private Network (VPN) to authenticate through the DISA Firewall using Pulse Secure. Once authenticated, users are required to use Secure Shell (SSH) software to connect to the server. See below for detailed instructions on accessing and initializing the OOB SSL VPN webpage and invoking PuTTY SSH software. Contact your local Network Administrator to ensure that TCP Port 22 is open for Basic Command Line access and Ports 8561 and 8591 are open for SAS Enterprise Guide access.

**Pulse Secure Download/Installation**

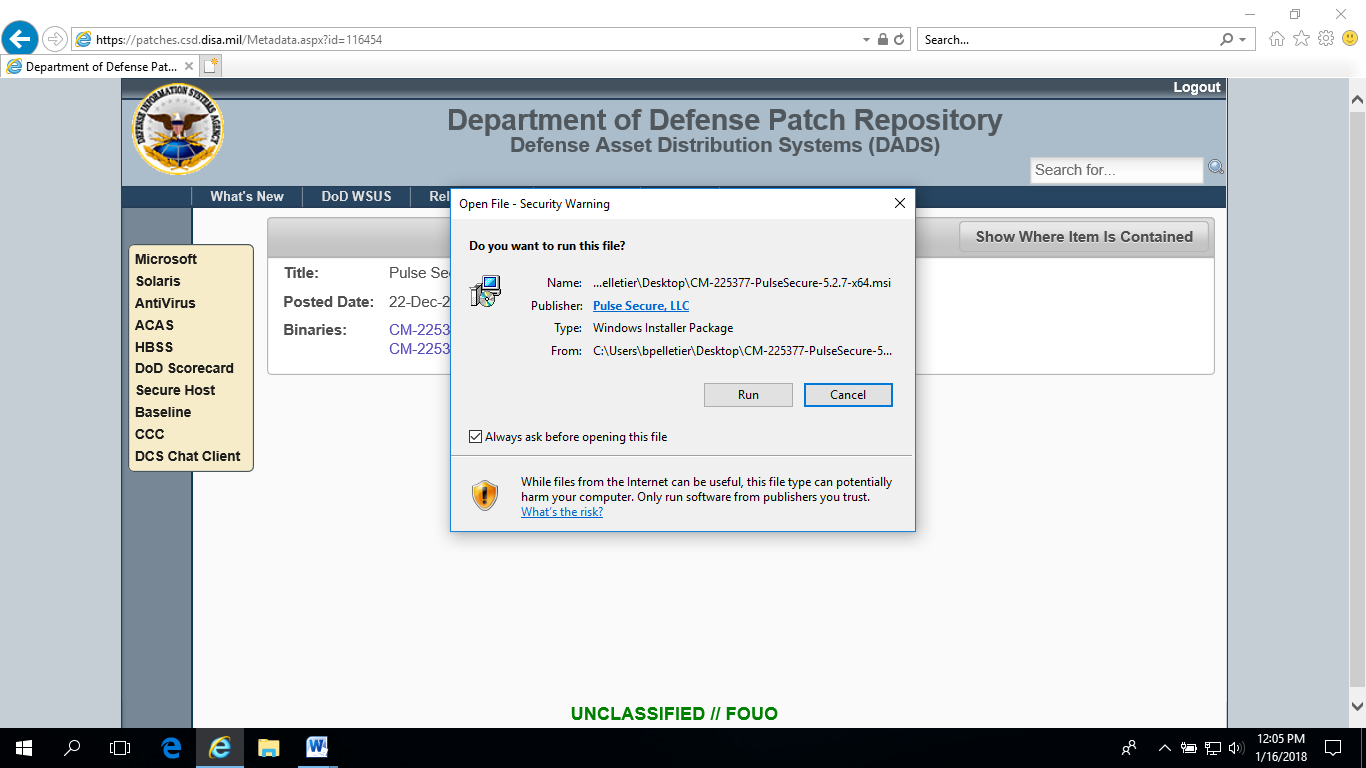
Go to <https://patches.csd.disa.mil/Metadata.aspx?id=116454>. Log on with your CAC (email signature).



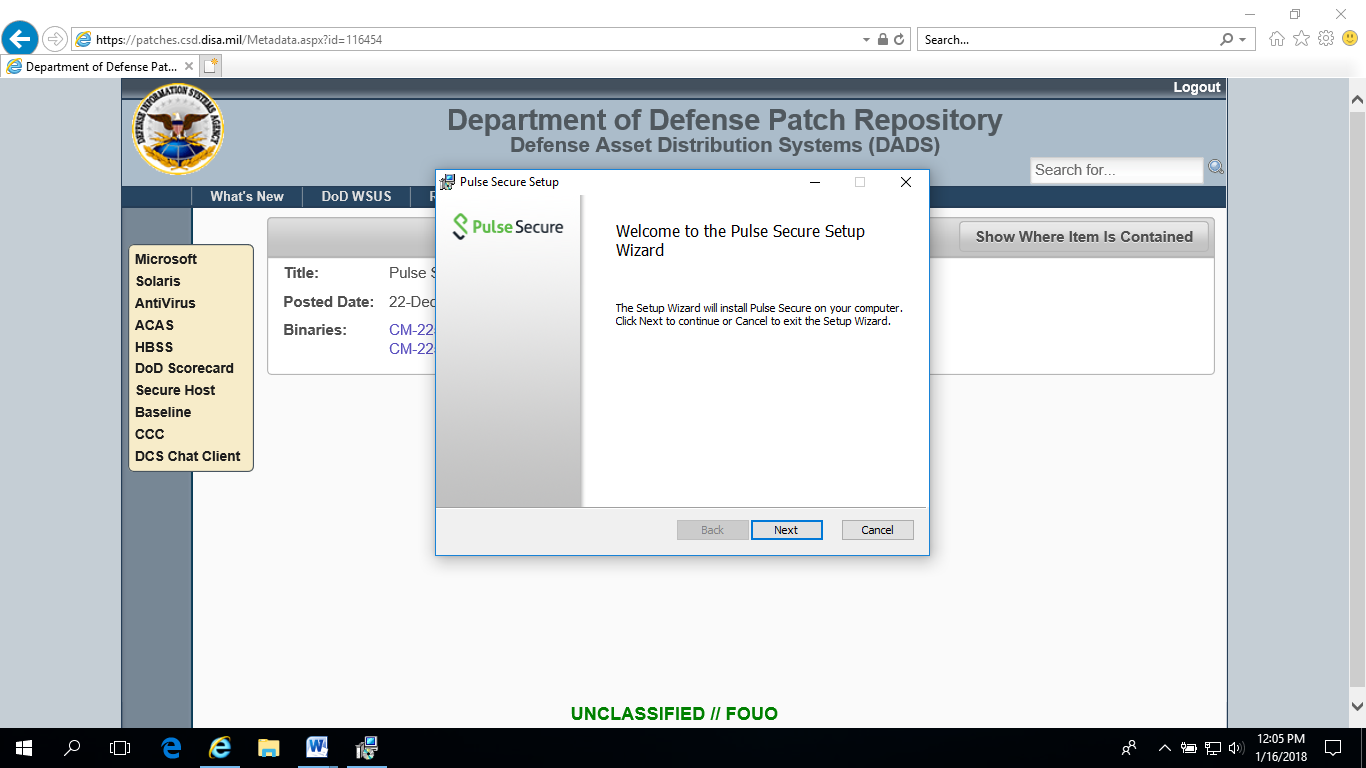
Choose CM-225377-PulseSecure-5.2.7-x64.msi (for 64-bit installation).



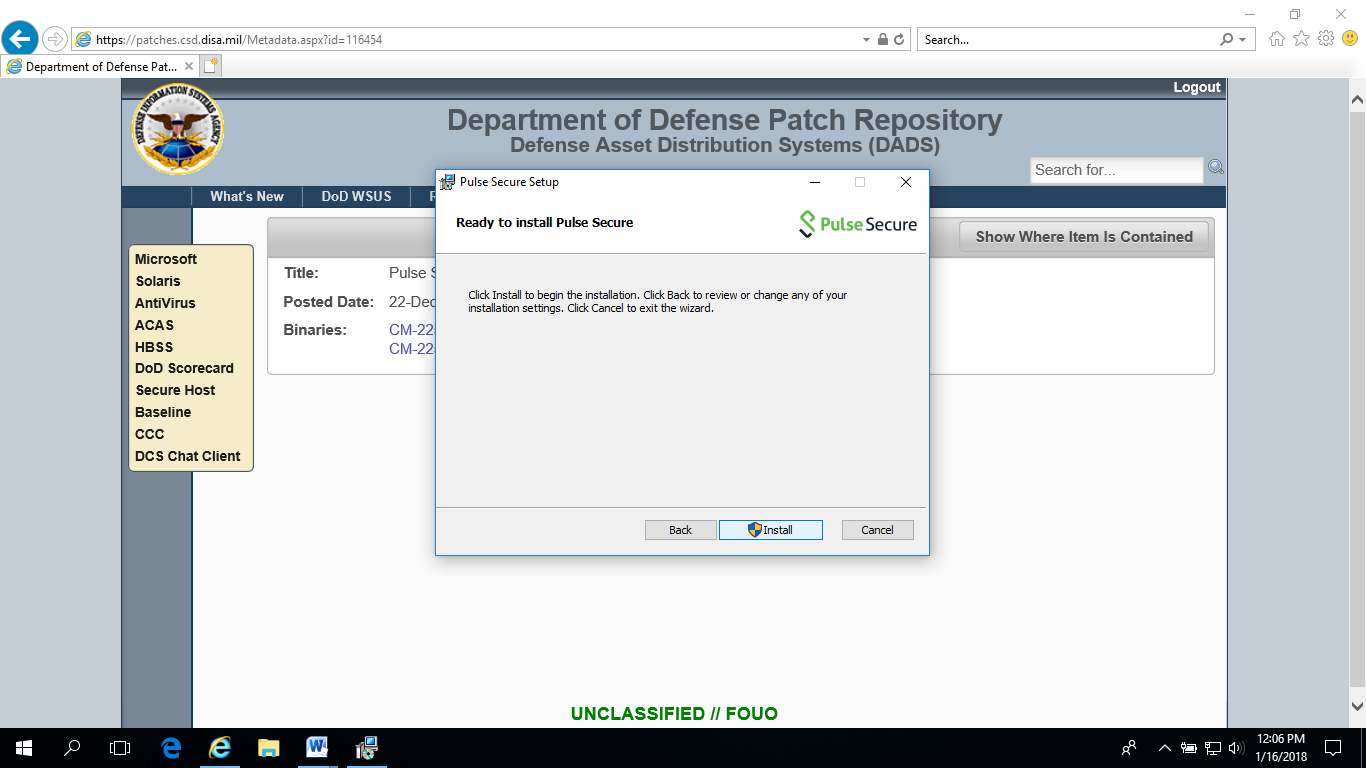
Run the installation.



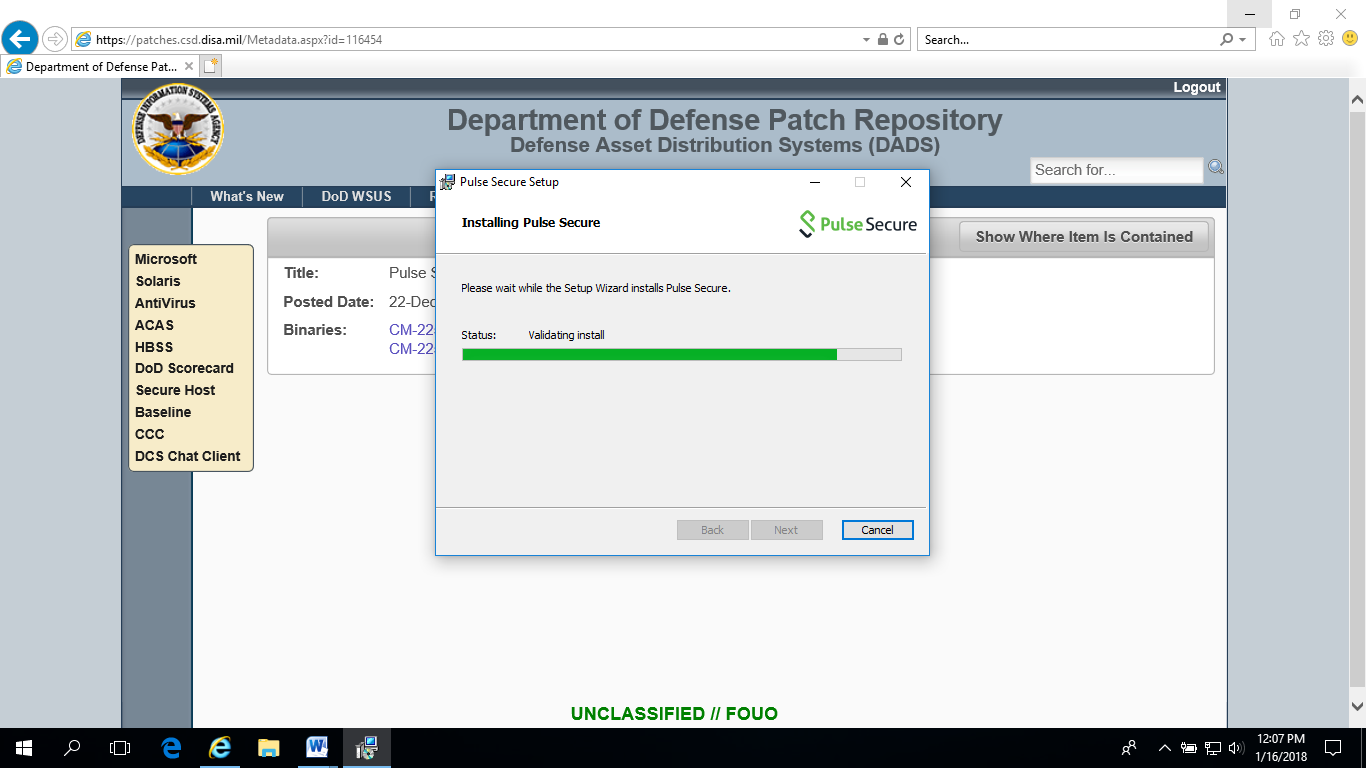
Click Run.

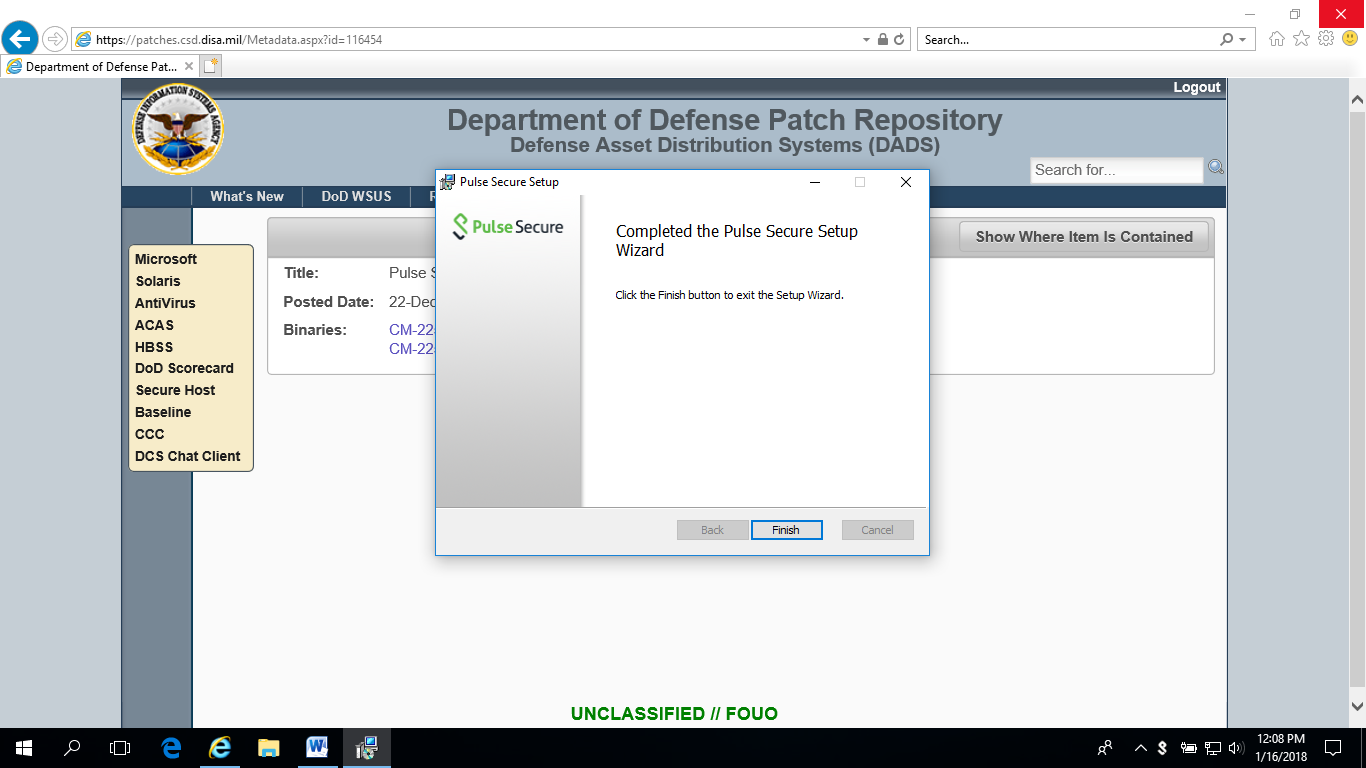


Click Next.



Click Install.

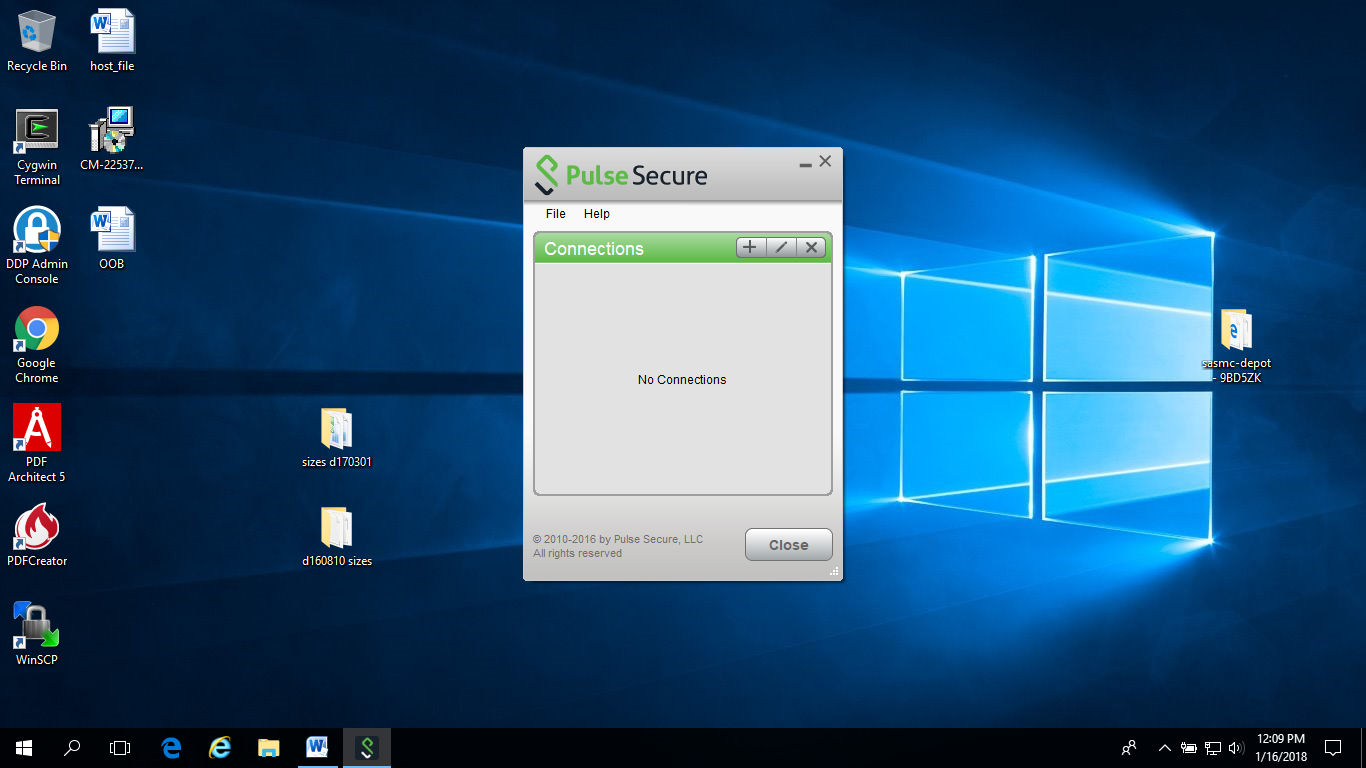




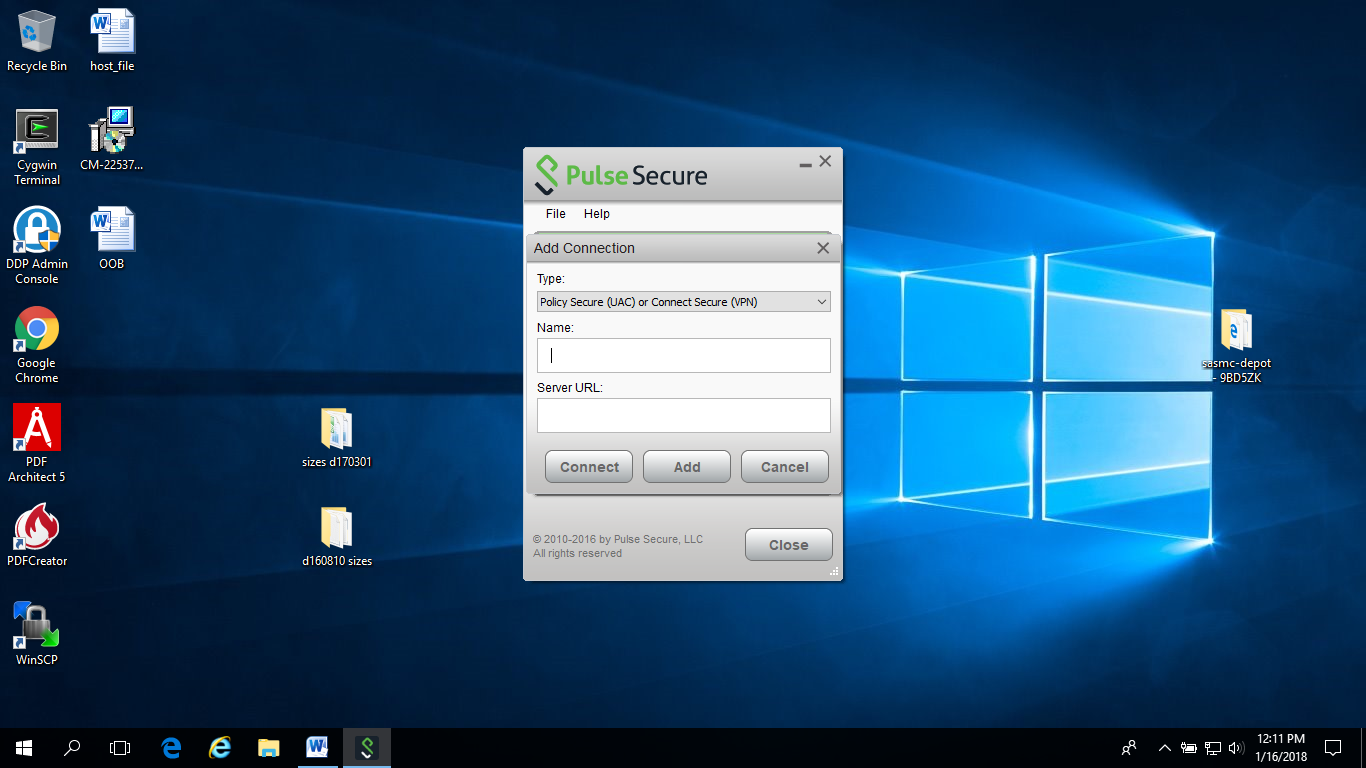
Click Finish.

Pulse Secure is now installed.

Open Pulse Secure



Click the ‘+’ to add a new connection.



Enter the information for one of the new OOB URLs. The Name can be anything that you like.

https://oobvpn-mech.csd.disa.mil

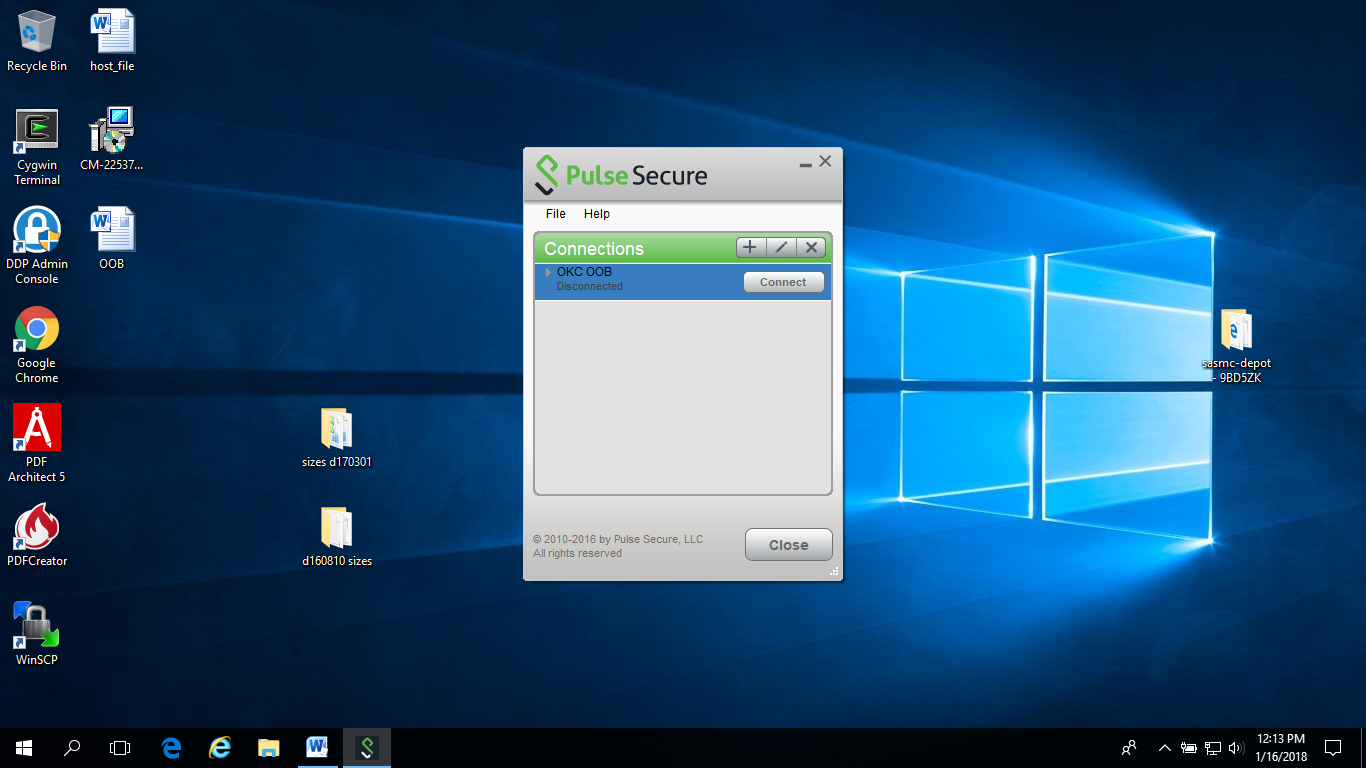
https://oobvpn-mont.csd.disa.mil

https://oobvpn-ogdn.csd.disa.mil

https://oobvpn-okco.csd.disa.mil



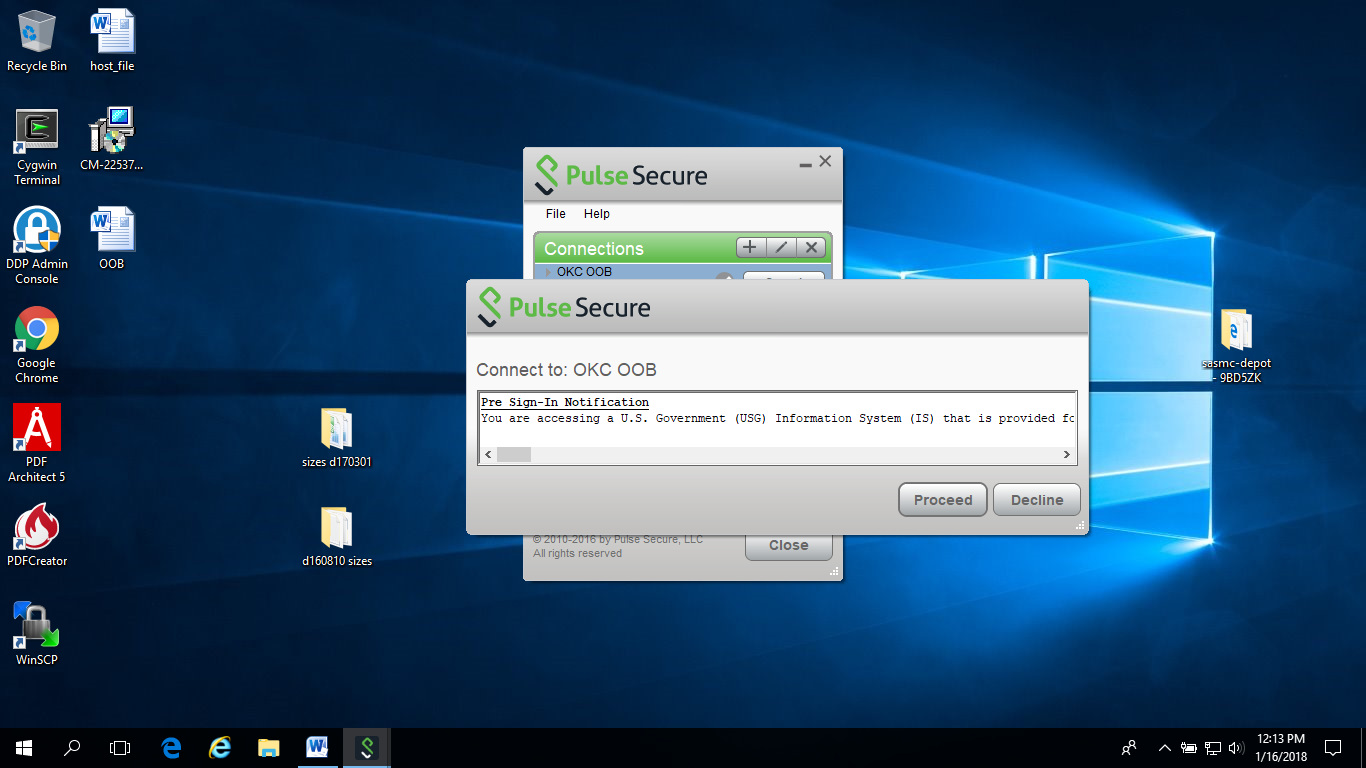
Click Add.



Repeat to add the other OOB URLs if wanted.

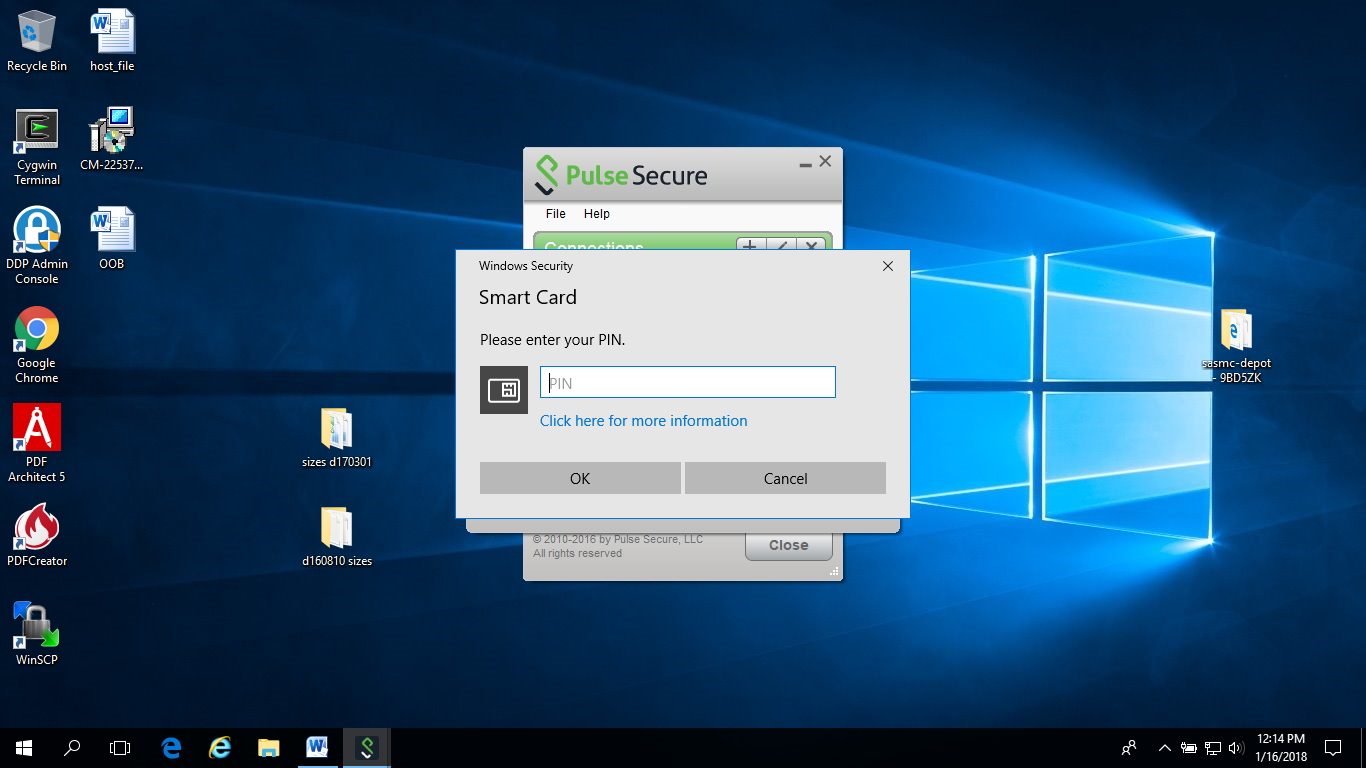
You are now ready to connect to the OOB.

Choose one of the connections that you have set up and click Connect.

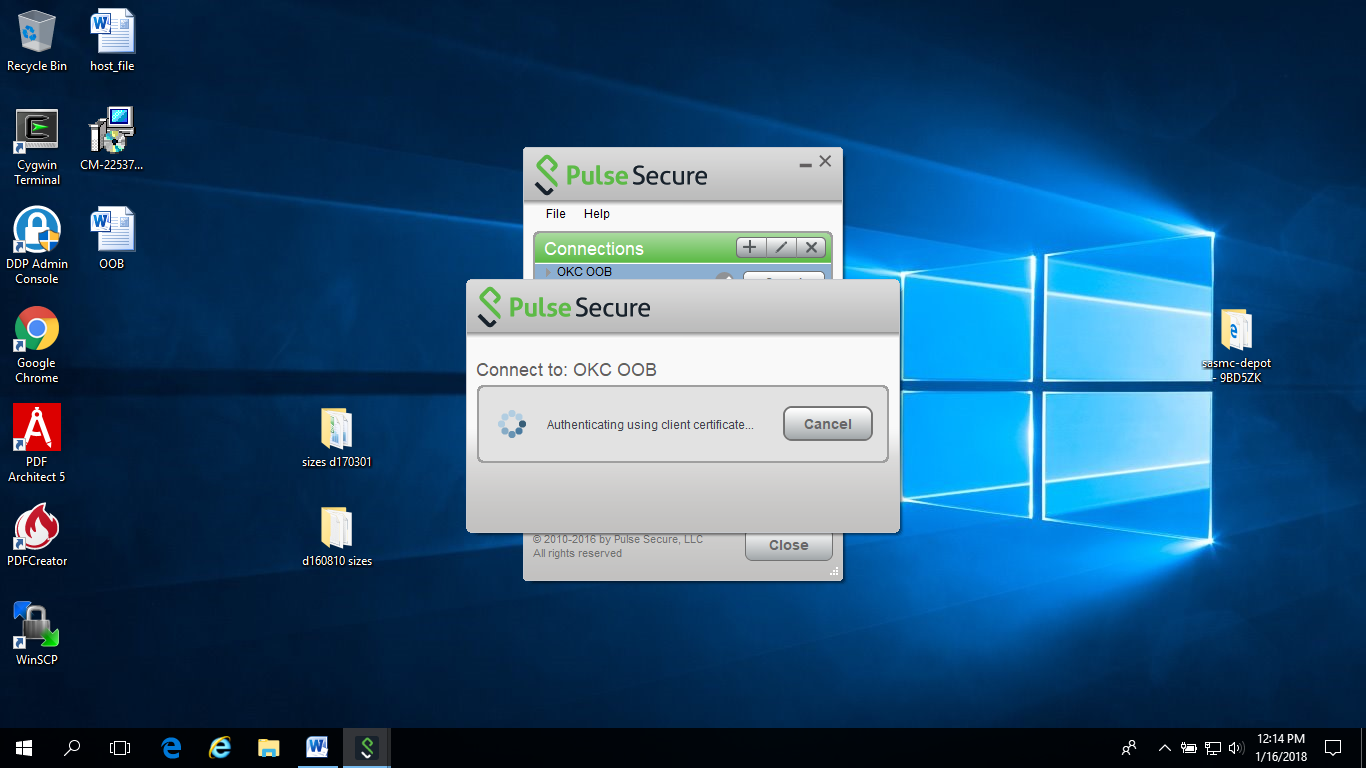


Click Proceed.

Choose your email certificate and click Connect.



Enter your pin.



## Secure Shell (SSH) Login

Once the account is approved and permissions set, users will be provided information about their SCE user ID, work space, and temporary password for accessing the system. Any SSH software with appropriate encryption ciphers can be used to access the SCE. Following are instructions for using PuTTY.

Downloading PuTTY

1. Go to the following website to download PuTTY:

[PuTTY Download at http://www.chiark.greenend.org.uk/~sgtatham/putty/download.html](http://www.chiark.greenend.org.uk/~sgtatham/putty/download.html) or open a ticket with your local helpdesk to have PuTTY installed on your machine.

2. Scroll down to the section titled, ‘The latest release version’ and find your operating system. Click on ‘putty.exe’ to download.

3. Save the executable to your workstation.

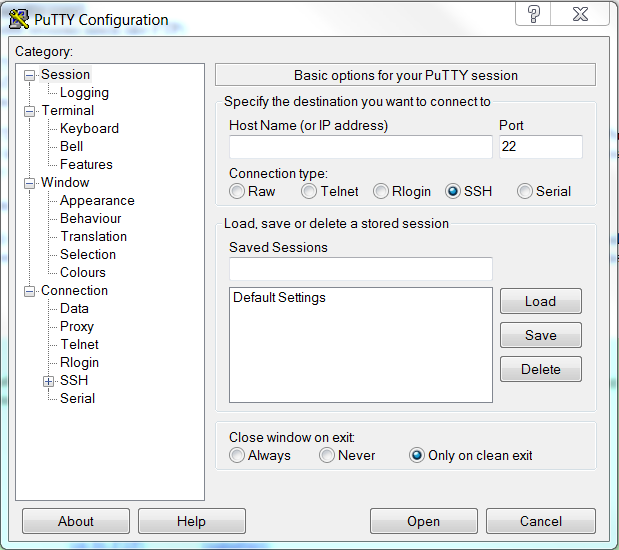
• PuTTY is a little larger than 350 KB in size.

• This is where you will invoke PuTTY in the future.

4. Once the download has completed successfully, double click the icon for “putty.exe”.

Initializing PuTTY

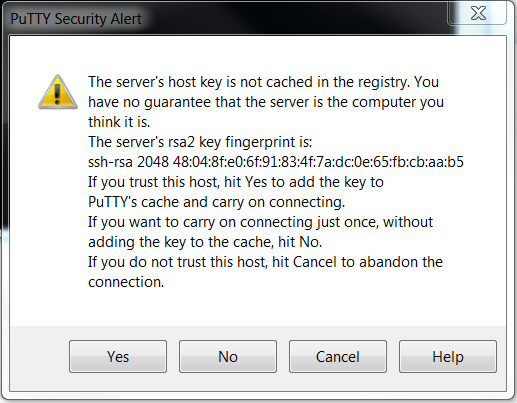
You will be presented with a PuTTY Configuration screen.



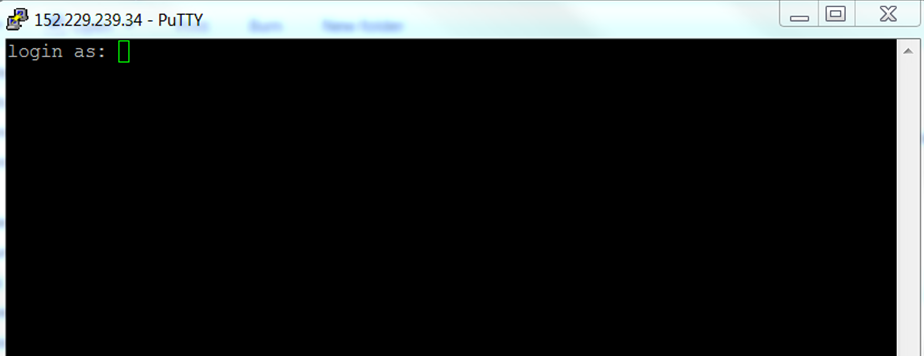
Enter the address in the host name, using the table below. Make sure the Port is set to 22 and the connection type is SSH. Save your session and name it something easy for you to recognize. If you use OOB before this step you’ll need to use the OOB IP address. Otherwise use the non-OOB IP Address.

|  |  |  |
| --- | --- | --- |
| Node Name | OOB IP Address (if connecting through OOB first) | Non-OOB IP Address |
| SCE | utinip1q | Submit a ticket to the DHA GSC ([dhagsc@mail.mil](mailto:dhagsc@mail.mil)) with your IP address to be verified. Once verified, you will be contacted with the public IP Address. |

Save your session then hit open or double-click on the session name. A box will appear asking if you trust this host.



Click yes. This will bring up a login/command screen.



Enter your login id. If you are logging on for the first time or your password has expired, it will prompt you for your old and new password. Your new password should follow these rules:

at least 15 characters

at least 2 uppercase alpha characters

at least 2 lowercase alpha characters

at least 2 numeric characters

at least 2 special characters

maximum of 2 repeated characters

minimum of 4 characters not in previous password

cannot use previous 20 passwords

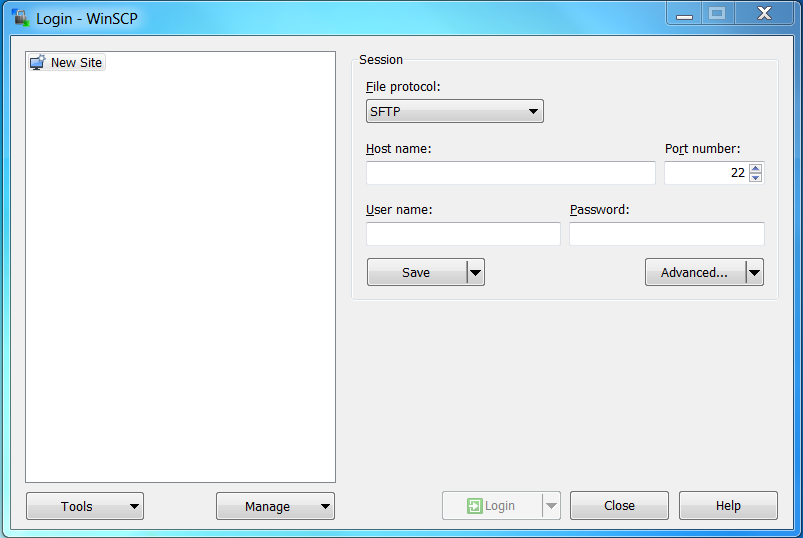
There is no message to notify you whether your password change was successful or not. Try the new password just one time. If it does not work, try the old password again and chose a different new password.

When you are done with PuTTY simply type exit and the session will exit, closing the window.

## Transferring Files to/from the SCE

Any secure transfer software with appropriate encryption ciphers can be used to access the SCE. Following are instructions for using WinSCP.

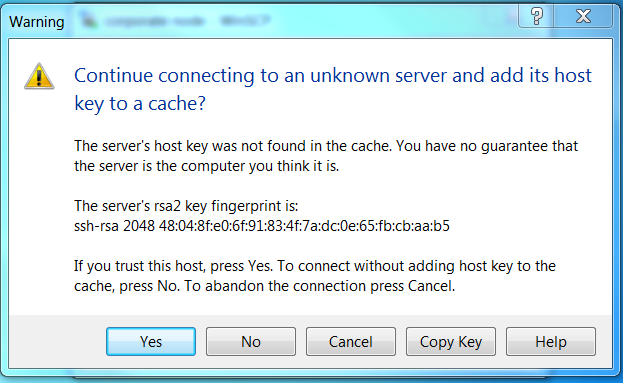
WinSCP can be used to transfer files from the SCE to your local computer. Go to the following website to download WinSCP (<http://sourceforge.net/projects/winscp/>), or open a ticket with your local helpdesk to have WinSCP installed. Once it is installed, go to the start menu and open the program to initialize it.



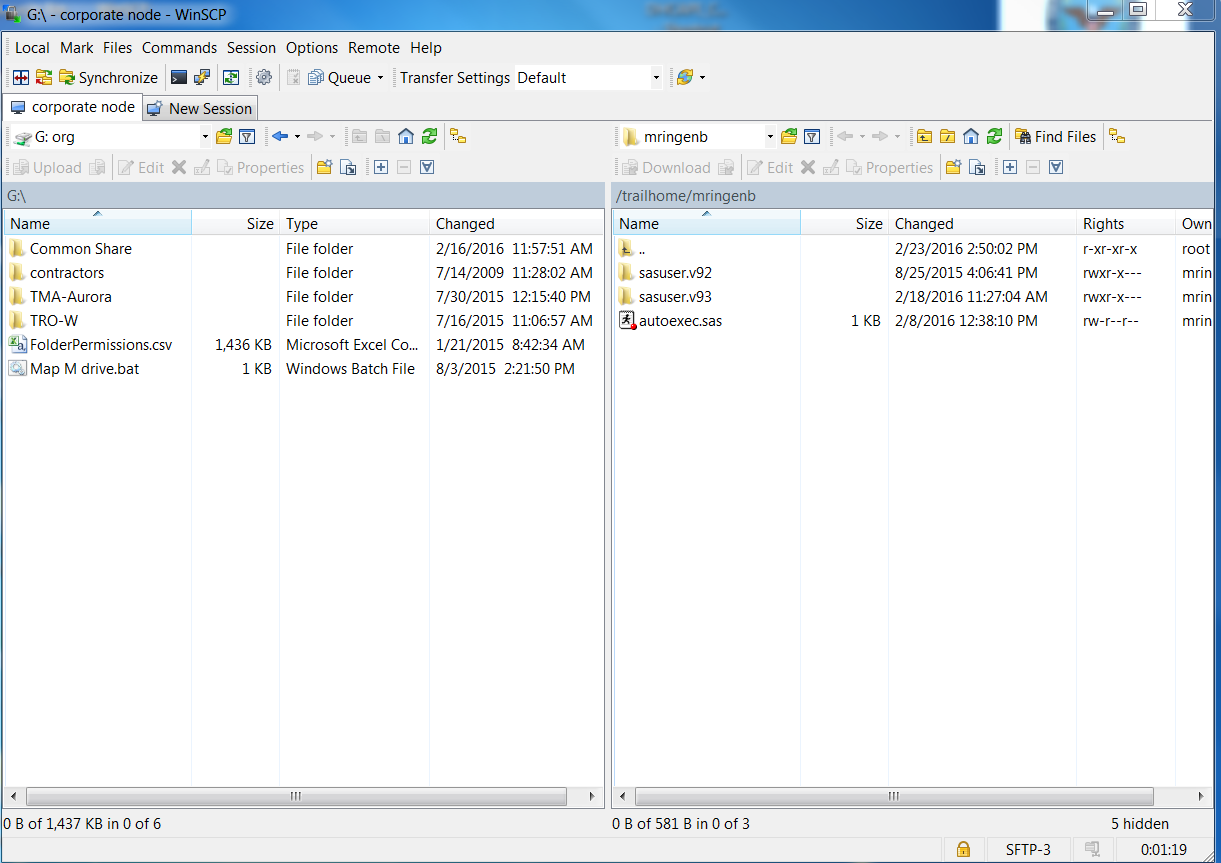
Make sure the file protocol is set to SFTP and the port number is 22. Then enter the IP address into the host name using the below table:

|  |  |  |
| --- | --- | --- |
| Node Name | OOB IP Address (if connecting through OOB first) | Non-OOB IP Address |
| SCE | utinip1q | Submit a ticket to the DHA GSC ([dhagsc@mail.mil](mailto:dhagsc@mail.mil)) with your IP address to be verified. Once verified, you will be contacted with the public IP Address. |

Enter your userid and click save. Name your sign in or save as default. It should autoconnect, and bring up this message asking if you trust this host.



Click yes and enter your password again. It will bring up a file transfer window you can use to move SAS programs from your local computer to the SCE, and data or logs from the SCE to your local computer. You can change directories using the drop down boxes, or by clicking on the folders to navigate. Drag and drop to move files.



## Submitting SAS Jobs in the SCE

SAS jobs run in the background on the SCE to prevent running jobs from failing if the VPN or SSH session times out. You may create or edit SAS programs on the SCE using the PICO or vi editor. If you prefer to work on your PC, you may edit your programs in Windows and then use a secure file transfer to copy them to the node.

Due to the high usage of the SCE, there is a limit of 3 programs per user running at a time. If you already have three programs running, you’ll need to wait until one finishes before setting off another SAS program. If more than 3 are submitted, the most recent submission may be cancelled without warning.

Important: In order for programs to run, they MUST be named with a .sas extension. To submit a SAS job:

1. Log on to the node using a SSH client and change to the directory where the SAS program is located in your file system space.

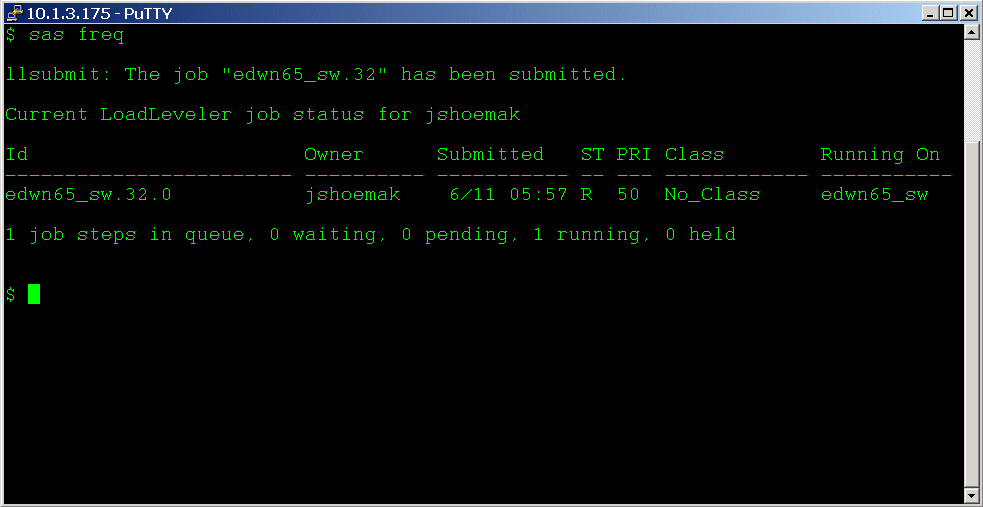
Example:

[utinip1q}:/home/userid > cd /hpae2/

***Note: Do not store code or data in your home directory, specifically /home/userid. Files in this area may be deleted without warning.***

1. Remember, if the macro described in Keeping Logs is used (page 8), you must use the syntax provided in that section to submit your programs.

sas <program\_name.sas> -altlog <program\_name.log>



Your program will be submitted through Load Leveler as a background process and run immediately. The SCE can have up to 25 jobs running at a time, with up to 16 normal, up to 10 big jobs and up to 6 dedicated jobs at a time. Any jobs after that enter a queue to be executed sequentially. Keep this in mind on busy days, and try to only run jobs you need when you see jobs waiting. You can see the queue by typing llq.

**Using Environment Variables**

Because Load Leveler is a batch scheduling application, any environment variable defined in the shell when Load Leveler is invoked will not be passed to the SAS program. In order to use environment variables in your SAS program, they must be defined by the SET option when SAS is invoked. This can be done using the following:

sas <program\_name> -SET <variable\_name> <value>

**SAS Temporary Workspace**

There are multiple SAS temporary workspace areas on the SCE. Please use the guidelines below and commands for using the appropriate SAS workspace and submitting SAS jobs.

**Table 4. Temporary Workspace Definitions**

|  |  |
| --- | --- |
| **SASTemporary Workspace** | **Combined Workspace**  **Requirements of:** |
| Small (Normal) | Less than 30 GB |
| Large (Big) | Greater than 30 GB |

**Commands for submitting SAS jobs on the Nodes**

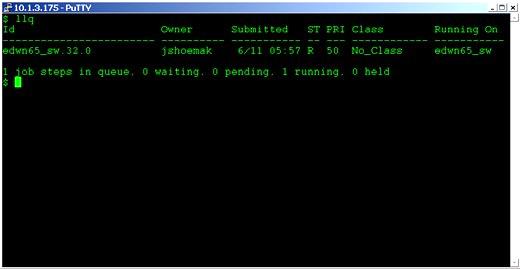
- To start a job running in the normal workspace, the command is **sas *jobname.sas***

- To start a job running in the big workspace, the command is **sasbig *jobname.sas***

- To determine what jobs are running in the SAS Temporary Workspaces simply type **'llq'** at the command prompt and look under "Class" to determine the jobs running or queued to run in the Normal, and Big SAS Temporary Workspaces.

**Checking Job Status**

To find the current status of running jobs, type llq at the command prompt.



All submitted jobs have completed when the output reads:

**llq: There is currently no job status to report.**

Check the .log files for results.

**Canceling a submitted Job**

To cancel a submitted job, use the sasstop command. It will list all the jobs you have currently running in the system and ask you which job you want to delete. If no jobs are running, it will inform you of that fact and exit.

To invoke sasstop on the SCE, type sasstop at the command prompt.

Note: sasstop will only allow a user to cancel their own submitted jobs. Jobs submitted by other

users are not shown in the list nor are able to be cancelled by non-owning user accounts.

Note: Sometimes SAS jobs which terminate abnormally leave residual data within the temporary

SAS work space. This data will be removed by the system administrator on a routine basis.

Remember, do not store programs, scripts, data, formats, etc. under your user home directory

/home/<userid>/. There is very limited space available for the home directories. If this space becomes full, all users will be locked out of the SCE. If the system administration staff sees files in the home directories other than those placed there by the staff, they will be removed after due diligence.

## Moving Files to the SCE from External Systems

SCE users may periodically require files be made available on the server that only exist on external systems and for which using WinSCP is not an option. Following are instructions for having a file(s) moved to the SCE.

1. Ship Tape(s) to SDD SCE Administration Staff

Coordinate with the external system source to have the file(s) written to DVD, CD-ROM, USB disk. Ship the media to the following address:

**SDD SCE Administration Staff**

**c/o Alqimi Technology**

**5203 Leesburg Pike, Suite 600**

**Falls Church, VA 22041**

If you need additional information, please contact [mdr.data.extraction@alqimi.com](mailto:mdr.data.extraction@alqimi.com)

2. Complete an *Import* Transmittal Form

Complete an Import Transmittal form by supplying the following information. The Import

Transmittal form may be found here: <http://health.mil/Military-Health-Topics/Technology/Support-Areas/MDR-M2-ICD-Functional-References-and-Specification-Documents>

**Section 1 - Requestor Information**

• Requestor Name & Company - The SCE user requesting the data and their company name.

• Requestor Information - The phone number and e-mail address of the requestor.

• Return the tape(s) - Does the tape(s) need to be returned to the source? Check the appropriate box. If the tape(s) does need to be returned, provide the shipping information such as POC, address and phone number.

**Section 2 - Media Characteristics**

• Media Type - Indicate the media format to be read (CDROM, DLT, IBM 3480, IBM 3490, or LTO).

• Total Number of CDs/Tapes – This is the total number of CDROMs/Tapes to be read in.

• For CD-ROM, DVD, and USB Drives, list the file names to be read in to the SCE.

• For Tapes, indicate the following:

–Application used to create the tape – i.e. tar, ReelExchange, NT Backup, etc.

–Data Format of the Tape(s) - ASCII or EBCDIC

–Label Type – ANSI, EBCDIC, or UNLABELED

–In this order, provide the file name, record format (fixed block=fb, variable block=vb), block size, line count, record length, and logical volume serial number.

For example, if you have one file named myfile, which is in fixed block format, contains a block size of 32,760, a line count of 54,980, record length = 196, and has a logical volume serial number = 770076, the Tape Transmittal would display the information as: **myfile : fb : 32760 : 54980 : 196 : 770076**

**Section 3 - File Characteristics**

• File Placement - Provide the SCE directory path of where the file(s) is to be placed. The requestor must have appropriate privileges to read and write files in this location.

• File Access Privileges: List the file access permissions (i.e. rwxrw----). These permissions will determine who has read, write, and execute privileges to the file(s).

**Section 4 - Authorization of Action**

• To Be Completed by SDD SCE Administration Staff

3. Send completed Import Transmittal to SDD

Send the completed Import Transmittal Form to the SDD SCE Administration Team via electronic mail - [mdr.data.extraction@alqimi.com](mailto:mdr.data.extraction@alqimi.com).

The SCE Administration Staff will ensure that the information is complete and accurate.

4. If USB Disk Drive, Ship to DISA

a. Drives must be shipped via Federal Express directly to DISA OKC. Two days prior to shipment, notify SDD of plans to ship the external media.

b. SDD will respond to your notice with a work “ticket number” to include on the FEDEX shipping label. This information must be included on the shipping label or the drive may get inappropriately routed within DISA.

c. Once you have a work “ticket number” the drive may be shipped to:

**Defense Information Systems Agency (DISA) – OKC**

**Tim Swinford / DISA Property**

**Bldg. 3900 / 8705 Industrial Blvd.**

**Tinker AFB – 73145**

**Phone POC: 405-855-8445 and/or 405-855-8393**

**Please mark/annotate attention: Tape Media Librarian(s)**

d. Notify SDD that the drive has been shipped. Provide the FEDEX Tracking number and Serial Number of the USB Disk Drive in this notification.

Upon receipt of the USB Disk Drive by DISA, it will be prepared for data upload.

SDD will not process an import request until both the Transmittal Form and media are in hand.

Upon reading the media, SDD SCE Administration Staff will perform minimal QC, which consists of verifying that the file(s) and byte count(s) read were consistent with the Import Transmittal Form. SDD will notify the requestor of the files placement in the specified location.

If necessary, SDD SCE Staff will coordinate the return of the media with the POC as indicated on the Import Transmittal Form.

## Copying Files from the SCE to External Media

SCE users may periodically need a file(s) that exists on the SCE copied to external media and shipped to a third party for analysis or fulfillment of contractual obligations. SDD is able to copy data to several types of external media. Choosing the type of external media is dependent on the size of the file(s) being copied and the technical abilities of the recipient organization.

|  |  |  |
| --- | --- | --- |
| ***Media Type*** | ***Maximum Size*** | ***Notes*** |
| CD | 700 MB | Files larger than the max. size may be split or compressed to accommodate the size limitation |
| DVD | 8 GB | Files larger than the max. size may be split or compressed to accommodate the size limitation |
| USB Disk Drive | Dependent on the size of the drive | Individual files must not be larger than  10GB in size. |

*Note: Thumb-drives are not permitted.*

SDD works with on-site DISA technicians to perform the data extractions.

Following are instructions for having a file(s) read to external media and shipped. Notes:

• The SCE user/requestor must have the appropriate permissions to view and extract the requested file(s).

• The data recipient, also referred to as third-party, must have a valid Data Sharing Agreement (DSA) on file with the TMA Privacy Office covering receipt and use of the data being extracted.

• The amount of time it takes to copy the data to external media is dependent upon the size of the file(s), accuracy of information contained on the Export Transmittal Form, the number of requests for exports in queue, and approval. SDD generally acts on data export transmittals in a “first-in, first-out” manner unless otherwise directed by DSD.

• SDD SCE Administration Staff will not manipulate (split or compress) files. Files to be copied to external media must be in their final format.

1. Complete an Export Transmittal form

Complete an Export Transmittal form by supplying the following information. The Export Transmittal Form may be found here: <http://health.mil/Military-Health-Topics/Technology/Support-Areas/MDR-M2-ICD-Functional-References-and-Specification-Documents>

**Section 1 - Requestor and Shipment Information**

Requestor Name - The SCE user requesting the data be cut to external media.

Requestor Company Name and DSA # - The SCE user company name and the Data Sharing Agreement (DSA) number which authorizes the work to perform extractions for the data recipient (note that the DSA # should match the DSA # that is listed on the user’s SCE AARF).

Project and Justification for Export - List the Project details which require that data be written to external media and sent to the recipient.

FEDEX Account Number (for shipping) – Provide a Federal Express account number for shipment of the external media to the recipient. The account number may be provided by the Requestor or the Recipient. The Requestor is also responsible to schedule pickup from DISA if USB media is used.

Requestor Contact Info - The phone number and e-mail address of the requestor.

Shipment POC and DSA # - The third parties name, phone number, and address of where the media should be shipped as well as the DSA number which authorizes receipt of the data.

Target Platform – Designate the system platform of the third party. What operating system will be used to read the media?

Media Type - Indicate the type of media to be created (CD, DVD, or USB Disk Drive).

**Section 2 - File Characteristics**

File(s) location - Provide the SCE directory path of where the file(s) is located.

File name(s) : line count : byte count - In this order, provide the file name(s) to be cut to external media, its line count, and file byte count. **myfile : 54980 : 1354900**

Record format: record length and field names (flag PHI fields) - In this order, provide the file record format, and record length. Include a list of field names as specified. **fb : 76**

**Section 3 – Media Characteristics**

To Be Completed by SDD SCE Administration Staff

**Section 4 - Authorization of Action**

To Be Completed by SDD SCE Administration Staff

2. Send completed Export Transmittal to SDD

Send the completed Export Transmittal Form to [mdr.data.extraction@alqimi.com](mailto:mdr.data.extraction@alqimi.com).

The SCE Administration Staff will ensure that the information is complete and accurate, coordinate creation of the external media, perform minimal QC by checking the byte count(s), and ship the media to a third party as defined on the Export Transmittal Form.

## Changing Your Password

AIX passwords expire every 55 days. The first time you log on after password expiration, you will be prompted to change it.

Following are the DISA requirements for passwords:

at least 15 characters

at least 2 uppercase alpha characters

at least 2 lowercase alpha characters

at least 2 numeric characters

at least 2 special characters

maximum of 2 repeated characters

minimum of 4 characters not in previous password

cannot use previous 20 passwords

There is no message to notify you whether your password change was successful or not. Try the new password just one time. If it does not work, try the old password again and chose a different password.

If you would like to change your password before it expires, you can do so using the ‘passwd’ command.

Accounts will be locked after 3 unsuccessful login attempts. If your account is locked because of too many unsuccessful login attempts, open a ticket with the DHA GSC ([dhagsc@mail.mil](mailto:dhagsc@mail.mil)). Be sure to include your user id and that you are trying to access the SCE.

If you have access to Purchased Care systems (TED, PCDW, etc.), your user id/password is the same as the SCE.

**Commonly Used UNIX Commands**

Following are some of the basic commands that you will need in the UNIX environment.

**Command Reference Table**

ls

The “ls” command lists files in a directory. There are many options you can use with the "ls" command. For example "ls -a" will list ALL of the files in a directory (files and directories whose name begin with a period are considered hidden files). "ls -al" will list ALL files in LONG format. Here is an example directory listing:

www:~> ls -laF

total 34

drwxr-xr-x 4 root other 2048 Sep 24 11:25 ./

drwxr-xr-x 102 root root 2048 Sep 24 11:24 ../

-rw-r--r-- 1 root other 384 Jan 6 1998 .bashrc

-rw-r--r-- 1 root other 383 Jan 6 1998 .cshrc

-rw-r--r-- 1 root other 706 Jan 6 1998 .defaults

-rw-r--r-- 1 root other 1858 Jan 6 1998 .emacs

-rw------- 1 root other 2797 Jan 6 1998 .history

-rw-r--r-- 1 root other 137 Jan 6 1998 .login

-rw-r--r-- 1 root other 138 Jan 6 1998 .logout

-rw-r--r-- 1 root other 232 Jan 6 1998 .mailrc drwx------ 2 root other 512 Jan 6 1998 Mail/ drwxr-xr-x 2 root other 512 Jan 6 1998 bin/

In this example, the first block of each row (-rw-r--r--) shows the type and permissions for an individual file within your current directory. The first column tells you the type of file: '-' means it is a normal file, 'd' means it is a directory, and an 'l' means it is a link to another file (much like a shortcut in Windows). The next nine positions show the file's Read, Write, and Execute permissions in blocks of three. The first three characters (often 'rw-') are the permissions for the owner of the file, the second three are group permissions, and the final three are permissions for anyone else besides the owner and anyone in the group.

The next column is a number representing how many physical links to the directory or file exist on the file system. Files generally have one link to them due to the fact that directories cannot link to files specifically. Notice that the directory up one level, '..', contains a large number of links (102) due to the number of home-directories that

reference it as '..'.

The next four columns contain the name of the owner of the file (equivalent to the first three 'rwx' permissions), the group owner (second three 'rwx'), the file size, file date, and file name. Note that by using the '-F' flag (must be a capital F), directories are marked with the / symbol, and the / is not actually part of the directory name. Also, files marked as executable are shown with the ‘\*’ symbol following the name (only when the -F flag is set).

cd

The “cd” command is used to change directories. The "cd /" will take you to the root directory of the file system tree; "cd /usr" will take you to the directory named 'usr' that is located off of the root directory; "cd mail" will take you into a directory called 'mail' off from your current directory (note the lack of ‘/’ before the directory name); and "cd .." will take you to the parent directory in the file system tree. Some command-line shells, such as "bash" or "tcsh" expand the ~ symbol to mean a person's home directory. You could then either type "cd ~" to change back to your home directory, or "cd ~anotheruser" to go into another user's home directory.

pwd

The “pwd” command prints/outputs your present working directory to standard output.

mkdir, rmdir

These commands are used to create and remove directories. The "mkdir class" will create a directory called class in your current directory. Whereas "rmdir class" will delete the directory named class. Note that "rmdir" only works on directories that do not contain any files.

cp

To copy a file, use the “cp” command. The syntax is "cp *source destination*", where *source* is a

source file and *destination* is either a file name or directory in which to place the file. For example, "cp /usr/local/seminar.c ." will copy a file located in '/usr/local' named 'seminar.c' to '.' which is the symbol that stands for your current directory. "cp /usr/local/seminar.c my.c" will copy the

‘seminar.c’ file to your current directory under the name 'my.c'.

mv

The “mv” command is used to move *and/or* rename a file. "mv my.c first.c" will rename a file

called 'my.c' to 'first.c'. Assuming that 'class' is a directory, "mv my.c class" would move the file

'my.c' into the ‘class’ directory. If 'class' is a file, this operation will instead delete 'class' and then rename 'my.c' as 'class', which is probably something you didn't want. You can also rename and move at the same time. For example, "mv my.c class/first.c" would move the file 'my.c' into the

'class' directory and rename it to 'first.c' all in one step.

rm

The “rm” command deletes, or removes, files from the files ystem. Typing "rm my.c" would delete the file 'my.c'. You can also use wildcards. For example, "rm my\*" will delete every file whose

name started with the word 'my', including 'my.c'. Unlike Windows, these wildcards can appear

anywhere in the file name, and do not need to be confined to the standard 8.3 notation used by MS-DOS. Directories and their contents can be deleted by using the '-r' flag which stands for recursiveness. For example, "rm -r class" would delete ALL files and directories under 'class' and

'class' itself regardless if the directory is empty or full.

cat, less, more, head, tail

These commands are used to view the contents of files. "cat" displays the entire file on the screen, regardless if your terminal can view everything at once (the top portion scrolls off, but can be retrieved by scrolling back in a window or sometimes by holding down the 'Shift' key and pressing 'Page Up'). "less" and "more" both display the contents of a file one full screen at a time. "head" is used to display the first few lines of a file, and "tail" is used to display the last few lines of a file. For example, "tail -25 my.c" displays the last 25 lines of the file 'my.c'. "cat first.c" would display all of 'first.c', and "more first.c" will display the file 'first.c' one screen at a time.

grep

Search a file for a particular pattern by using the “grep” command. "grep" stands for Get Regular Expression Pattern. This command searches a file for all lines matching a particular pattern and prints those matching lines on standard output. For example, "grep fun my.c" prints every line of the file ‘my.c’ that contains the word 'fun'.

man

The “man” command brings up the UNIX Manual Pages for a particular command. For example, to learn about the rest of the options for the "ls" command, type: "man ls"

w, who, whoami, id

These commands are used to find out the list of users currently logged into the system and what they are doing. "w" provides slightly different output than "who". "whoami" returns the username of the person currently logged in. "id" prints your User ID, and Group ID, and a list of all the groups you have access to.

chmod

The “chmod” command is used to change the permission bits, called mode, on a file or directory. Only the owner of a file or directory and the superuser can change the permission bits/mode. See the “ls” command for information on viewing a file or directory mode.

Every file and directory is assigned nine permission bits that comprise the mode. The mode is used to determine what operations may be performed on a file and by whom. The mode consists of Read, Write, and Execute bits in blocks of three (Execute is also called “search” when referring to a directory): one block for the owner of the file or directory, one block for the group that the file or directory belongs to, and one block for others. Each user will fit into only one of the three blocks/categories.

For files, the read bit allows the file to be opened and read. The write bit allows the contents of the file to be modified or truncated. The execute bit allows an executable file to be executed.

For directories, the combination of read and execute (aka “search”) bits allows the contents of the directory to be listed. The combination of write and execute bits allows files within that directory to be created, deleted, and renamed. Having only the execute bit will allow the directory to be entered but not have any of its contents listed.

File or directory modes may be changed using octal notation or symbolic format. The octal notation format is described below. The basic syntax for the “chmod” command is:

chmod <octal or symbolic notation of read, write, execute permissions> <file or directory name>

The octal notation format sets file or directory permissions based on three octal numbers. The first number defines access for the user, the second number for the group, and the third number defines access for others. Each of the three numbers is a combination of permission bits. The octal notation is between 0 and 7.

Use the UNIX command CHMOD to change access permissions by summarizing the numerical values for Owner, Group and Other.

|  |  |
| --- | --- |
| **Digit** | **Permissions** |
| 0 | None |
| 1 | Execute only |
| 2 | Write only |
| 3 | Write and execute |
| 4 | Read only |
| 5 | Read and execute |
| 6 | Read and write |
| 7 | Read, write, and execute |

Examples:

#1) chmod 770 tedn.sas - allows owner and group to have read/write/execute privileges, other no privileges

#2) chmod 764 tedn.sas - allows owner read/write/execute, allows group read/write only, allows other read only

Using the “ls –l” command, example #1 and #2 above would appear as such:

#1) rwxrwx--- example1 groupname 2567 Sep 10 12:15 tedn.sas

#2) rwxrw-r-- example1 groupname 2567 Sep 10 12:15 tedn.sas

ps

The “ps” command is used to find the Process Status of all processes currently running on the machine. Typing "ps" without any options lists all programs currently running in your process group. “ps ux” or "ps -ef" lists all of the processes on the machine (Some UNIX versions prefer

one method over the other. If one way does not work, try the other). Combining the "ps" and "grep" commands through a pipe can give you a list of all the processes you have running, and can be done like this:

ps aux | grep <yourusername>

The '|' symbol, called a pipe, takes the results of the first command (in this case, "ps -aux") and uses it as input to the second command ("grep yourusername"). Let’s take a look at an example:

winds:/dsk0> ps ux

USER PID %CPU %MEM VSZ RSS TTY STAT TIME COMMAND

root 1 0.0 0.1 1048 112 ? S 0:03 init [3]

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| gandalf | 521 | 0.0 | 0.0 | 1652 | 0 tty2 SW | 0:00 | [bash] |
| gandalf | 652 | 0.0 | 0.7 | 1668 | 672 tty4 S | 0:00 | -bash |
| gandalf | 672 | 0.0 | 0.0 | 1516 | 0 tty4 SW | 0:00 | [startx] |
| gandalf | 677 | 0.0 | 0.0 | 2224 | 0 tty4 SW | 0:00 | [xinit] |
| gandalf | 4481 | 0.2 | 1.6 | 4104 | 1560 pts/0 | S 0:00 vi commands.html | |
| gandalf | 4452 | 0.0 | 1.0 | 1652 | 1012 pts/3 | S 0:00 -bash | |
| gandalf | 4545 | 0.0 | 0.9 | 2496 | 936 pts/3 R | 0:00 ps ux | |

The first column contains the user ID of the owner of that process. The second column contains the PID, or Process Identification number. The next two columns show the percentage of CPU Time and Memory the process has consumed during its entire running life. The next two columns show the Virtual Size of the program (total size of all memory in use) and how much of that memory is currently resident in the computer at the moment. Thus, the RSS number is usually much less than VSZ, because data are either shared, or is marked unused and are swapped to disk to free up room for other processes to use resident memory.

TTY shows which terminal the process is currently running on. Usually, tty1 through tty6 are processes controlled by a user at the main console (ALT-F1 through F6 to switch), and pts/# are processes from either inside X-Windows or through telnet in the network. STAT corresponds to the type of process status running at the time: 'R' means the process is currently active (as is the case for our “ps” command gathering the process data), 'S' means the process is sleeping, 'W' means the process is waiting for a signal to trigger swapping from disk and back into memory (note the 0 Resident Set Size), and 'Z' stands for a zombie process (see below). TIME shows the total amount of time the process has taken up CPU. In this case, each process except 'init' has taken up trace amounts of CPU, while 'init' has taken 3 seconds since the computer was started.

The last column of the "ps" command output contains the name of the process. The name can be represented in several different ways depending on the state of the process. If the name begins with a '-' symbol, such as '-bash', then it is recognized as a login shell. If the name is surrounded by [ ]'s, then the process is currently swapped out of memory to disk (with an RSS of zero).

Zombie Processes. Processes marked 'Z' occur during a coding error on behalf of the programmer to not properly *wait* for one of its children to exit after a *fork* call in the C language ("man" pages are available for both of these functions). Such processes are marked <defunct> and will only terminate when their parent process (PPID) exits.

kill, killall

Force a process to exit or terminate by using the “kill” command. This command is used to send signals to processes, most commonly the signal to kill a process (hence its name). Looking back at the "ps" example, to kill the "vi" process, you can type "kill 4481". Only programs that do not block the Terminate signal can be killed in this fashion. You instead must specify the “kill”

command using a '-9' as the first argument to the prompt. For example, to kill the unused,

swapped out 'bash' process, type: kill -9 521

The "killall" command behaves in the same way as "kill", only each process matching the name you give it will be sent the signal. To kill all of your "bash" programs (and consequently kick yourself back to the login prompt), type:

killall -9 bash

Note: If you own a process that is using close to 99% of the CPU, it is generally a good idea to "kill -9" it, as it most likely won't respond to normal signal handling. The system PID 1, "init", can never be killed.

Note: Do not use kill to kill a SAS job, use the sasstop command.

at

The “at” command reads from standard input the names of commands to be run at a later time and allows you to specify when the commands should be run. The “at” command mails you all output from standard output and standard error for the scheduled commands, unless you redirect that output. It also writes the job number and scheduled time to standard error. When the “at” command is executed, it retains the current process environment. It does not retain open file

descriptors, traps, or priority. The syntax for the “at” command is:

at [ -c | -k | -s | -q Queue ] [ -m ] [ -f File ] { -t Date |Time [ Day ] [Increment ] }

For example, if user *jdoe* wants to run a sas job called jobname.sas from a fictitious common directory at 11:30pm on August 15th, the command would be as follows:

/common/jdoe/jobname.sas at 2330 Aug 15 <enter>

sas jobname.sas <enter>

<ctrl-d>

For more information about different options and techniques on the formation of the “at”

command, reference the man pages.

compress

The “compress” command compresses data using adaptive Lempel-Zev coding to reduce the size of files. When possible, a compressed file replaces the original file, specified by the file parameter, with a .Z appended to its name. The compressed file retains the same ownership, modes, and modification time of the original file. If no files are specified, the standard input is compressed to the standard output. If compression does not reduce the size of a file, a message

is written to standard error and the original file is not replaced. Files being compressed must have

correct permissions to be replaced. For example, to compress the ‘foo’ file and write the percentage of compression to standard error, type:

compress -v foo

The foo file is compressed and renamed foo.Z.

For more information about different options and techniques on the formation of the ‘compress’

command, reference the man pages.

uncompress

The “uncompress” command restores original files that were compressed by the “compress”

command. Each compressed file specified by the file parameter is removed and replaced by an uncompressed copy. The uncompressed file has the same name as the compressed version but without the .Z extension. If the user has root authority, the expanded file retains the same owner, group, modes, and modification time as the original file. If the user does not have root authority, the file retains the same modes and modification time, but acquires a new owner and group. If no files are specified, standard input is expanded to standard output. For example, to uncompress the foo.Z file, enter:

uncompress foo.Z

The foo.Z file is uncompressed and renamed foo.

## UNIX File Naming Conventions

**Absolute Naming**

Within the UNIX directory structure there are two ways to name any file: relative naming and absolute naming. An absolute name, or absolute path as it is often called, specifies exactly where in the file system the particular file is. It tells the whole name of the file, starting at the root of the file system. An absolute name starts with /, the root, and names each directory along the path to the file, separating the directories with /. This is very similar to DOS, except for the direction of the slash and the fact that there is no disk drive designation. As an example, the absolute name for your mailbox might be /home/iris2/class9/mbox. The ‘pwd’ command always reports an absolute pathname.

**Relative Naming**

The second way to name a file in UNIX is with a relative name. Whereas an absolute name specifies exactly where in the file system a particular file exists, a relative name specifies how to get to it from your current directory. The look of a relative name may vary a lot. Depending on your starting directory there are a number of paths to a particular file.

In the simplest case, just naming a file in your current directory is a relative name. You are specifying how to get to this file from your current directory, and the path is to just open the file in the current directory.

When using relative paths, the special directories ‘.’ and ‘..’ that are contained in every directory are used frequently. Recall that ‘.’ specifies the directory itself, and ‘..’ specifies its parent. So, if the file mbox is contained in your current directory, naming the file with ./mbox and mbox are equivalent. The special directory ‘..’ is used to name a directory at the same level in the tree as your current directory, that is, a sibling of your current directory. The following example illustrates using ‘..’ to look at a sibling directory.

% pwd

/home/iris2/class9

% ls

NewBibligraphy.refer bibs mbox

ShortFile bin src

baby.1 ig.discography unix.refer

% cd bin

% ls

pwgen

% ls ../src

helloworld.c pwgen.c

**Short-cuts for File Naming**

Since certain file naming patterns are used over and over, UNIX provides some short-cuts for file naming. Actually, it is the shell that provides these, but the distinction is not critical at this point. In particular, very many file accesses are either to your own home directory or to the home directory of another user. To make it easier to point to these places, the ~ character is used. Alone, ~ refers to your home directory. So the file ~/mbox refers to the file mbox in your home directory. Likewise ~ username refers to the home directory of that particular user. So,

~dickson/mbox refers to the file mbox in the user dickson's home directory.

**File Naming Limitations**

UNIX allows you great flexibility in naming your files. Older System V Release 3 systems limited the length of a file name to 14 characters. Berkeley Unix systems, as well as newer versions of System V have substantially relaxed this limitation. Many systems allow the name of individual files to be up to 256 characters, and the maximum absolute pathname to be about 1023 characters. This means that files can be given meaningful names quite easily. Also, since UNIX is sensitive to the case of the file names, you can use mixed-case names to add clarity. While long, meaningful names can be quite nice, it is also possible to go overboard with file naming. So, try to give your files meaningful names, but try not to overburden yourself or others that have to access the files with overly long names.

**File Name Extensions**

While UNIX does not actually have the same notion of a file extension as is found in some other systems, notably DOS, many user and applications programs behave as it did. UNIX does not consider the ‘.’ character any differently than any other character in a file name. However, applications programs often use it to add an extension to a file name that specifies something about the contents of the file. These extensions sometimes tell what programs were used to create a file. If more than one was used, and is needed to decode the file, multiple extensions are used. Typically, the extension will tell what language the data in the file is in. A good example of this is the C compiler. It assumes that its input files will have an extension of ‘.c’. Its executable output generally has no extension, unlike DOS which uses an .EXE extension for executables. If we have a program called hello.c, its executable version is likely to be called just hello.

## The UNIX Directory Tree

Files in UNIX are stored in directories, which are organized into a tree type configuration. At the top of the tree is the root, called /.

Locations in the directory tree are called paths, and are specified as a list of directories separated by a '/'. Barney’s home directory, for instance, is in the home directory, which is in the root directory, and therefore the path is "/home/barney".

If you leave off the leading "/", the path is assumed to start in the directory you are currently in, for instance if you are in "home", "barney/songs" would be the directory songs contained in Barney's home directory. You can also use "..", which specifies the parent directory of the one you are in "../etc" from home would be the "/etc" directory.

There are a few standard directories you will find in pretty much all UNIX systems.

*/bin* This contains the basic system commands.

*/etc* This contains system configuration files and programs used for administrating the system.

*/lib* This contains the system libraries.

*/tmp* This is used to store temporary files.

*/usr/bin* This contains all the commands not in /bin.

*/usr/man* This contains manual pages for programs.

*/usr/local* This contains local programs, that where installed by your sysadmin and not included with the original system. In particular, /usr/local/bin is local

binaries and /usr/local/man is local man pages.

*/home* The location of this varies greatly from system to system, but somewhere on the system will be a place where all the home directories are, including yours.

## Getting Around Directories

You have been given a directory in which you can store your personal files, called your *home directory*. When you log in to the system, this is where you start off. You probably don't have any directories to start off with. If you want to create a directory underneath your home directory, use the *mkdir* command. For instance, to create a directory to hold your programs, type ‘*mkdir programs*’.

Now you have a directory you can get into with the *cd* command. For instance, to get into your *programs* directory, type ‘*cd programs*’. To get back to your home directory from anywhere, simply type ‘*cd*’. To go up a directory, type ‘*cd ..*’.

If you want to copy or move a file into a directory, use the *cp* or *mv* command as normal, but instead of specifying a destination file, specify a directory. For instance, if you type ‘*cp helloworld.c programs*’ from your home directory, it will copy the file *helloworld.c* into your *programs* directory.

To remove a directory, use the *rmdir* command. Note that the directory must be fully empty to do this. To remove your *programs* directory, change to that directory using the ‘*cd*’ command and type ‘*rm \**’. This deletes all files in that directory so make sure you are in the right place! You can find out where you are by typing ‘*pwd*’. Now that all files have been deleted, you can delete the directory. Go back to your home directory and type ‘*rmdir programs*’.

# Appendix A: The PICO Editor (For editing in UNIX) and VI editor

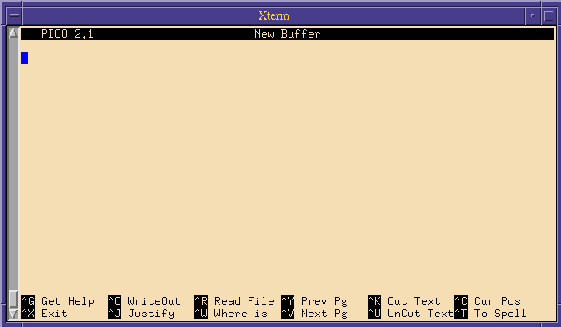
PICO Editor

(http:/[/ www.ncsu.edu/cc/essentials/managing\_files/text\_editors/pico\_tutor/index.html)](http://www.ncsu.edu/cc/essentials/managing_files/text_editors/pico_tutor/index.html))

PICO is a line-mode text editor used to create files, reports and letters. You will need a line- mode editor if you use your account on a non-X Windows computer.

To start using PICO, enter ‘pico filename‘ at the system prompt where filename is either the name of the file you want to edit (one that already exists) or the name of a new file you want to create. If you do not provide a file name, PICO will open a new file but it will be unnamed until you save it.

The screen for a new file will look something like this:



In the list of commands at the bottom of the PICO screen, caret (^) stands for the control (ctrl) key. ‘^G’ means to hold down the control key and press the letter ‘G’. PICO commands are always a combination of the control key and another key. After you enter a PICO command you do not need to press the return key.

Quitting PICO

Press ‘^x’ to quit or exit the PICO editor. PICO will prompt you with a message asking if you want to save your changes. ‘Y’ saves the changes and ‘N’ quits PICO without saving what you've done since the last time you saved.

Entering Text

At the system prompt, type ‘pico’ to create a new file. You should see PICO in your window. The top line of your screen is called the status line. It shows what version of PICO you are using, the file name (it will say New Buffer if it hasn’t been named yet), and whether or not you have made changes (Modified will be in the upper right corner of the PICO screen if something has been entered but not saved). At the bottom of the screen are two lines showing the commands available for your use.

Now that you have an empty file, you can start typing. PICO automatically starts a new line when you run out of room (called "wrapping text," "text wrap," or "autowrap") so you do not need to watch the screen while you type. Press [return] when you want to start a new line. If you want a blank line between lines of text or data, press [return] twice.

Saving the file

Now that you have a file with something in it, this is a good time to save your work. You should save your files often, if for no other reason than strange things can happen and sometimes do. The common sense rule is to save often enough so that if you lose your work you will not have much to re-do. Some people recommend saving every 15 minutes.

To save a file, use ‘^o’, which stands for write out because you are writing what you have done to a file as output. When you press ‘^o’, PICO will prompt you for the file name. If the file does not have a name yet, you will need to type one in. If the file does have a name, it will follow the file name prompt, and all you need to do is press [return].

You may also save the file during the process of quitting PICO. ‘^x’ quits PICO after prompting you to save the file. Press ‘Y’ to save the file. Pressing ‘N’ will return the file to the state it was in the last time you saved it (if you had not saved the file during this editing session, the file will return to the state it was in when you opened it). If you alter a file and want to save the original version as well as the modified version, enter ‘Y’ to save the file. When you are prompted for a file name enter a new file name.

Editing in PICO

You can easily edit short files using only the following keys:

• [ret]: Inserts a new line in the file.

• cursor (arrow) keys: The four arrow keys move the cursor up, down, left and right.

• backspace/delete key: Deletes the character preceding the cursor.

Cutting text

Cutting or deleting text is a major component of any kind of editing. PICO gives you two ways to cut text: (1) cut a character at a time, or (2) cut a line at a time (unfortunately, you cannot cut a word at a time).

To delete a character, place the cursor on the character you want to delete and press ^d. Pressing your keyboard's delete key (some keyboards label it backspace) will delete the character preceding the cursor.

To delete an entire line, place the cursor anywhere within the line and press ‘^k’ (for kill or cut text). The entire line will be cut. If you change your mind about deleting the line before you delete another one, you may press ‘^u’ to bring back the line. The restored line will be placed wherever the cursor is.

Pasting text

Since ‘^u’ lets you restore the cut line wherever the cursor is and not just to wherever it came from, you may use ‘^k’ and ‘^u’ to "cut and paste" text. In PICO, you move blocks of text similar to if you were using a word processing package. You first need to mark (highlight) the text you want to move. Cut the text, move the cursor to where you want the text inserted, then paste it. Position your cursor at the beginning of the first line of the text block you want to move. Press

‘^^’ (ctrl-shift-6 key). Move the cursor to the end of the block you want to cut. The text should then be highlighted. Once the block is highlighted, press ‘^k’ to cut the text. Place the cursor to

where you want the text placed, and press ‘^u’ to paste. The text should then appear.

Reformatting text

To justify or reformat a paragraph (fill in gaps left by starting a new line) press ‘^j’. PICO defines paragraphs as text surrounded by blank lines or indentation. However, if you had a blank line between each line of text pressing ‘^j’ would not affect the text.

If you do not like the result of the justification, press ‘^u’ to "unjustify" the paragraph before you move the cursor outside the paragraph. Once you have justified text, the ‘^u’ command function changes from undelete to unjustify. However, when you move the cursor from the justified paragraph, the ‘^u’ command function returns to undelete. Therefore, if you need to unjustify the paragraph, you must do so before you move the cursor outside the paragraph.

To join lines that are separated by blank lines use ‘^k’ to delete the blank line and ‘^j’ to fill the paragraph.

Searching your PICO file

If you are proofreading a file by looking at a printout, it may be tricky to find the specific line you want to revise. An easy way to get to the right point in your file is to use PICO’s search, or

‘where is’ command, which is ‘^w’. This command lets you enter a character(s) or word(s) to search for, and then moves the cursor to the first occurrence. PICO begins the search from the

point in the file where the cursor is located. So, if the cursor is at the beginning of the second paragraph, the search begins at the beginning of the second paragraph.

To find a specific character or word, press ‘^w’ (for where is). A black strip with the word

‘search:’ will replace the two lines of commands at the bottom of the screen. You should then type the character(s) or word(s) you want to find. This search command is not case sensitive.

This search command is also not limited to finding only whole words. For example, if you were

to tell PICO to find “th”, it would find “that”, “the”, “they”, and “thick”, etc.

Using the spellchecker

PICO has a spellchecker that will check spelling in your text files.

To start the spellchecker, press ‘^t’. The PICO spellchecker compares the words in your file to words that are in its dictionary. When it finds a word that is not in its dictionary, it sends the prompt ‘Edit a replacement:’ followed by the misspelled word. If the word is correct, just press return. If the word is misspelled, you may change it by backspacing over it (to delete it) and then typing the correct word. You may also use the cursor and delete keys to edit parts of the word.

Inserting a file into PICO

To insert an existing file into the PICO file you are currently editing:

• Locate the cursor where you want to place the inserted file

• Press ‘^r’. After you press ‘^r’, you will receive the prompt ‘Insert file:’

• Type in the name of the file you want to insert and press return. The inserted file's contents will be inserted at the cursor.

This command does not delete or in any way alter the file that is to be inserted (a copy of the file is inserted).

If you change your mind about inserting the file after you have pressed ‘^r’, when prompted for the file name enter any character string that does not correspond with a file. The system will attempt to process the command, but when it does not find a corresponding file it will cancel the command and your text will not be altered. You will, however, receive the message ‘No such file:’ followed by the character string you entered.

Control keys for moving around in a file

If for some reason you cannot use cursor (arrow) keys, you may use the following commands to move around in your file.

• ‘^p’ moves to the Previous line.

• ‘^n’ moves to the Next line.

• ‘^f’ moves Forward a character.

• ‘^b’ moves Backward a character.

Clearing the display

If your display becomes cluttered (most likely because of interactive messages), you may clear or refresh it by entering ‘^l’. The messages are erased from your screen and the file you are working with remains.

Command list for PICO

The commands you can use in PICO are listed across the bottom of the screen. Remember, ‘^’

symbolizes the control key. ‘^G’ means to hold down the control key and press G.

^G Help. More information on the commands.

^X Exit PICO

^O Save a PICO file

^J Justify text within a paragraph. This command will fill in paragraphs that are missing, etc.

^R Insert an existing file into PICO.

^W Find a word or character string in the PICO file.

^Y Go back to the previous page.

^V Go to the next page.

^K Cuts the line of text where the cursor is located.

^U Uncuts the last text cut.

^C Gives you the exact location of your cursor within the file.

^T Run the spell checker.

When you have selected ^O to save a file or ^R to insert a file, you will be prompted for a file name. You will also be given the following new options:

^C Cancels the command.

^T Gives you a list of files in your home directory. If you select a file that already exists, PICO will ask you if you want to overwrite the file.

## Basic VI Editor

Beginning Your Editing Session

To edit a file vi [ filename ] To recover an editing session vi -r [ filename ]

Notes on vi commands and modal editing

All vi commands are entered in command mode. To enter command mode, press the ESC key. Some vi commands cause vi to enter another mode. For example, the i (insert command) causes vi to enter insert mode after which all keystrokes are inserted as text. To return to command mode from insert mode, press the ESC key. The :set showmode command will cause vi to display the current editing mode in the lower right corner of the editing screen.

Controlling the Screen Display of Your Session

Repaint the current screen {^l}

Display line #, # of lines {^g}

Moving the Cursor

Beginning of current line 0 or ^

Beginning of first screen line H

Beginning of last screen line L

Beginning of middle screen line M

Down one line j, {return}, +

End of current line $

Left one character h, {ctrl-h}

Left to beginning of word b, B

Right one character l, {space}

Right to end of word e, E

Right to beginning of word w, W

Up one line k, -

Beginning of next sentence )

Beginning of previous sentence (

Paging Through Text

Back one screen {^b}

Down half a screen {^d}\

Down one screen {^f}

Forward to end of file G

Move cursor to specified line line no.G

Up half a screen {^j}

Special Pattern Characters

Beginning of line ^

End of line $

Any character except newline .

Any number of the preceding character \*

Any set of characters (except newline) \*

Creating Text

Append text after cursor a Append text after end of line A

Insert text before cursor i Insert text at beginning of line I Open new line after current line o Open new line before current line O

Take next character literally (i.e. control characters...) and display it {^v}

Ending Your Editing Sessions

Quit (no changes made) :q

Quit and save changes ZZ, :wq

Quit and discard changes :q!

Using ex Commands From Within vi

Copy specified lines :co, t Display line numbers :set nu Disable display of line numbers :set nonu Move lines after specified line :m

Read file in after specified line :r filename Review current editor options :set Review editor options :set all

Set new editor option :set option

Write changes to original file :w

Write to specified file :w filename

Force write to a file :w! filename

Some Useful ex commands for use in vi

Some useful set options for your ~/.exrc file:

:set all Display all Set options

:set autoindent Auto magically indent following lines to the indentation of previous line.

:set ignorecase Ignore case during pattern matching.

:set list Show special characters in the file.

:set number Display line numbers.

:set shiftwidth=n Width for shifting operators << and >>

:set showmode Display mode when in Insert, Append, or Replace mode.

:set wrapmargin=n Set right margin 80-n for autowrapping lines (inserting newlines).

0 turns it off.

Searching Through Text

Backward for pattern ?pattern

Forward for pattern /pattern

Repeat previous search n

Reverse direction of previous search N

Show \*all\* lines containing pattern beg,endg/pattern/p

Example

:1,$g/compiler/p Will print all lines with the pattern compiler.

Substitute patt2 for all patt1 found. :beg,ends/patt1/patt2/g

Example

:%s/notfound/found/g Will change all occurrences of ‘notfound’ to ‘found’.