



United States Antarctic Program

Computer Requirements for Connecting to the USAP Network

Raytheon
Polar Services

The United States Antarctic Program (USAP) addresses U.S. federal government security and operational requirements for computing systems by screening all computers (including science experiments, mission operation systems, workstations, PCs, servers, laptops, and portable notebooks) prior to connecting to the USAP network. The following system requirements and operating system specifications apply to all equipment that will connect to the USAP network. These requirements are aligned with the *NSF Computer Security Policy*. Please direct inquiries to the USAP Help Desk at (720)568-2001 or helpdesk@usap.gov.

To minimize wait time for computer screening, please ensure your system meets the following requirements prior to deployment. Failure to comply with the following guidelines may result in excessive delays or a denial of access.

A computer system has to continuously maintain compliance with the computer requirements. A system that falls out of compliance such as falling behind in anti-virus definitions, patches, or vulnerability remediation may be disconnected without notice if NSF determines there is an unacceptable level of risk or threat to the USAP environment.

System Requirements

- **Administrator Access**
Obtain administrator username and password for computers prior to deployment. Screening technicians must have the authority to log on to the computer at an administrator level to accurately review the system configuration and run screening software. If the administrator username and password are not available, the screening process, as well as the ability to connect to the USAP network and its resources, will be delayed.
- **Connectivity**
Participants must provide all the equipment necessary to connect the computer system to the USAP network, including the Network Interface Card (NIC), external dongles or attachments used by the NIC, device drivers, etc. All equipment must be in working order.
- **Antivirus**
For computers running McAfee antivirus software, the Admin ID and password are needed to configure the software to update automatically from a local USAP server. The USAP IT division can provide current DAT files for McAfee and Norton users. All other antivirus software users must ensure proper updates are installed and the computer is virus free prior to deployment.
- **Patches**
Computers running an operating system (OS) must include the most current patch level of the OS, including the latest security patches.

- **Client and Server Software**
 - Client software used for the purposes of email and web browsing, and other client software, such as SSH and SFTP, are permitted.
 - Software that is not permitted for use on the USAP network includes:
 - Peer-to-peer (P2P) software, e.g., KaZaA, Skype
 - Email server software that provides SMTP/POP port services
 - Web server software that provides HTTP/HTTPS/FTP services
 - Network management servers, such as DNS and SNMP

Operating System Specifications

Operating systems must meet the following criteria to pass the computer screening process. All operating systems should be currently supported by the vendor. If the OS is not in one of the following categories, connection to the network must be evaluated at a USAP location by an IT technician before connecting the system to the USAP network.

- **Apple**
 - Mac OS version X, or later
 - Current antivirus software with latest virus definition files (DAT files)
 - Current patches installed and active for the operating system.
 - Current vulnerabilities remediated.
- **Linux**

RedHat Linux version 5, Fedora version 10, or later.

 - Current antivirus software with latest virus definition files (DAT files)
 - Current patches installed and active for the operating system.
 - Current vulnerabilities remediated.
- **Microsoft**
 - Windows XP, 2003, 2005, 2008, or later.
 - Current antivirus software with latest virus definition files (DAT files)
 - System32/wins folder does not contain “dllhosts.exe” or “svchosts.exe”
 - Current patches installed and active for the operating system.
 - Current vulnerabilities remediated.
- **Other Operating Systems, Embedded Systems, and Appliances**
 - Proactively work with USAP IT several months in advance of deployment to design your science support requests or mission support requests and get a preliminary connection determination.
 - Ensure that you have a current commercial off the shelf (COTS) operating system that is secure, robust, and can withstand continuous security, maintenance, and network management.
 - Current antivirus software with latest virus definition files (DAT files)
 - Current patches installed and active for the operating system.
 - Current vulnerabilities remediated.
- **Virtual Machines (VMs), Dual-Boot, Multi-Boot Systems**

These systems must meet the requirements for each operating system on the equipment as listed above.

Computer Screening Process

Screening technicians gather the following information during the computer screening process. Users using the USAP network without a screening rating of *Pass* are in violation of USAP information security policy and may be denied access to the USAP network. A *Fail* rating indicates the system owner is responsible for remediating the system before connecting to the USAP network.

Data Collected By Computer Screening	
<ul style="list-style-type: none">▪ User name▪ Date of check▪ Computer make and model▪ Computer affiliation (personal, grantee, NSF, other)▪ NSF Tag number (if applicable)▪ Computer hostname▪ OS version▪ OS patch level	<ul style="list-style-type: none">▪ Service pack/service release level▪ Serial number▪ MAC address▪ Wireless MAC address▪ Antivirus software▪ Virus DAT file date▪ Pass (computer cleared to connect to network) or Fail (computer needs remediation)

Computer screening is performed at the following locations.

- **Denver, Colorado (Orientation) and Christchurch, New Zealand (Clothing Issue)**
Computer screenings are performed for USAP personnel at orientation in Denver and for all deploying participants at clothing issue in Christchurch. Computers that receive a *Pass* rating within two weeks of deployment may connect to the USAP network upon arrival.
- **McMurdo and South Pole Stations**
Computer screening at McMurdo or South Pole station is only required for computers that did not received a *Pass* rating when screened in Denver or Christchurch within two weeks of deployment. If a computer arrives on station without being screened or having failed a screening, the system owner must contact the McMurdo or South Pole station Help Desk.
- **Marine Research Vessels (LMG or NBP)**
IT personnel perform screening onboard vessel during the port call or within the first two days at sea.
- **Palmer Station**
Computer screening at Palmer station is only required for computers that did not received a *Pass* rating when screened on vessel. If a computer arrives on station without being screened or having failed a screening, the system owner must contact Palmer Station IT personnel for screening prior to connecting to the network.