National Aeronautics and Space Administration

October 2007

remote connectivity guide

www.nasa.gov

NASA HQ Remote Connectivity Guide

Document Revision History

Status (Baseline/Revision/ Admin Change/ Canceled)	Document Revision	Effective Date	Description
Baseline	1.12-29	December 29, 2006	First draft printed and distributed for comment.
Revision	1.1-31	January 31, 2006	Second draft printed and distributed for comment.
Revision	1.5-17	May 17, 2007	Third draft; removed sections on Government Forms and Teleworking Long Term. Reordered content for better organization. Inserted additional material on VoIP phones.
Final	1.8-17	August 17, 2007	Final draft; changed document title to Remote Connectivity Guide. Removed appendices and reordered content for better organization.

Produced by the NASA Headquarters Information Technology & Communications Division, (ITCD).

For comments or questions about this document, please contact Michael Barrett, NASA Headquarters Telecommunications Manager.

The most current version of this document will be available for download at http://www.hq.nasa.gov/itcd/telework.html.

Table of Contents

1 Remote Access Options 8
1.1 Dial-in Connectivity 8
1.2 High Speed Connectivity (DSL, Cable Modem, Fiber Optics) 9
2 Frequently Asked Questions (FAQ) 11
3 Getting Help 13
3.1 Phone Tree for (202) 358-HELP (4357) 13
3.2 Hours of Availability 13
3.3 Getting Help Web Page 14
4 Websites to Bookmark 15
5 IT User Workplace Responsibilities 17
5.1 Maintaining the Security of Your Home Computer is Your Responsibility 17
5.1.1 Threats 17
5.1.2 The Defenses 18
5.2 Securing Sensitive Information at NASA HQ 20
5.3 Security Concerns: Computer Incidents 24
5.4 How to Change Your HQ Domain Password 25
5.4.1 For PC Users at HQ 25
5.4.2 For Macintosh OS X Users at HQ 26
5.4.3 For Remote Users (PC or Mac) 27
5.5 Frequently Asked Questions 28
5.6 Appropriate Use of IT Resources 29
5.7 IT Prohibited Practices 29
5.8 What is a Virus? 30
5.8.1 Virus Products and Information 31
5.8.2 Virus Response 31
5.8.3 Antivirus Software 31
6 VoIP Phone 32
6.1 Accessing Your Voice Mail Account 32
6.2 Activating the Call Forward Feature 32
6.3 To Deactivate Call Forwarding 35
6.4 How to Change Your CallManager Password 36
7 Accessing HQ IT Services 37
7.1 Internet Connection Using a Home Computer 37
7.2 Internet Connection Using a NASA-Issued Laptop 37
7.3 SecurID Token - Resetting the PIN 38
7.4 Virtual Private Network (VPN) 40
7.5 Using the Cisco VPN Client for Windows 40
7.5.1 When I'm connected, what access do I have? 42
7.5.2 How do I access my network files? 42
7.6 Using Cisco VPN for Mac OS X 46
7.6.1 When I'm connected, What Access Do I Have? 47
7.6.2 How Do I Access My Network Files? 48
7.7 Known Issues with the VPN Method of Accessing HQ 51
7.8 Secure Nomadic Access (SNA) 51
7.8.1 Logging On 51

7.8.2 Accessing Windows Files (U, W, X Network Drives) 52
7.8.3 Creating Bookmark Folders 53
7.8.4 Add Personal Bookmarks 54
7.8.5 Opening Files 55
7.8.6 Uploading Files 55
7.8.7 Deleting Files 58
7.9 SNA Frequently Asked Questions 58
7.10 Dial-Up 60
7.10.1 Windows XP Remote Access 60
7.10.2 Known Issues with Dial-In Method of Accessing HQ 61
7.10.3 Disconnecting from the NASA HQ Dial-Up Network 62
7.11 Macintosh Remote Access (Dial-In) 62
7.12 Shared Drives 62
8 Outlook Web Access (OWA) 63
9 SharePoint 65
9.1 How to Add SharePoint to Trusted Sites in Internet Explorer 65
9.2 Using the SharePoint Document Library 66
9.2.1 Working with Documents Libraries in SharePoint 73
9.2.2 About SharePoint Document Check Out and Check In 75
9.2.3 Edit a document 75
9.2.4 Restore a document to a previous version 77
10 WebEx 79
10.1 Setting up Meeting Manager on your Computer 79
10.1.1 Setting up Internet Explorer 6.x 79
10.1.2 Setting up Meeting Manager for Windows and Macs 81
10.2 Joining Meetings 83
10.2.1 Registering for a meeting from an e-mail message 85
10.2.2 Adding a meeting to your calendar program 87

Disclaimer Statement

No data shown in illustrations represents any “real” account, project, or individual. Any resemblance to actual accounts, projects, or individuals is purely coincidental.

About This Guide

NASA Headquarters (HQ) supports working remotely in an emergency as a contingency response that may be activated under certain circumstances. This guide provides instructions on how to remotely access the HQ network and computing resources, and can be used for teleworking on either an episodic or core basis.

For more information about NASA HQ Policy on teleworking, visit:

http://www.hq.nasa.gov/office/codec/sop/telecommute.doc

1 Remote Access Options

There are four ways to remotely access NASA HQ IT Services:

- **Virtual Private Network (VPN)**
- **Secure Nomadic Access (SNA)**
- **Dial-In**
- **Outlook Web Access (OWA)** - OWA can be used in combination with any of the other connection methods.

1.1 Dial-In Connectivity

- From a home computer:
  - **Outlook Web Access (OWA)**
  - **Secure Nomadic Access (SNA)**
    - WebTADS
    - Travel Manager
    - NASA HQ Intranet
    - Access Network Drives
    - Upload Files
- From a NASA-issued laptop:
  - **Outlook Web Access (OWA)**
  - **Secure Nomadic Access (SNA)**
    - WebTADS
    - Travel Manager
    - NASA HQ Intranet
    - Access Network Drives
    - Upload Files
  - **Outlook/Entourage E-mail and Calendaring**
  - **VPN**
    - WebTADS
    - Travel Manager
    - NASA HQ Intranet
    - Access Network Drives and Shared Applications
    - Upload Files

Note: When using Dial-in, the connection speed is very slow which may cause some applications to time-out.

1.2 High-Speed Connectivity (DSL, Cable Modem, Fiber Optic)

- From a home computer:
  - **Outlook Web Access (OWA)**
  - **Secure Nomadic Access (SNA)**
    - WebTADS
    - Travel Manager
    - NASA HQ Intranet
    - Access Network Drives
    - Upload Files
- From a NASA-issued laptop:
  - **Outlook Web Access (OWA)**
  - **Secure Nomadic Access (SNA)**
    - WebTADS
    - Travel Manager
    - NASA HQ Intranet
    - Access Network Drives
    - Upload Files
  - **Outlook/Entourage E-mail and Calendaring**
  - **VPN**
    - WebTADS
    - Travel Manager
    - NASA HQ Intranet
    - Access Network Drives and Shared Applications
    - Upload Files

Note: For full functionality, it is recommended to use a NASA-issued laptop for remote access.

Table 1.1 outlines the technical requirements for each method.

Table 1.1 Technical Requirements for Accessing HQ, By Method	
High-Speed	**VPN** ✓ A NASA-issued laptop. ✓ A High-Speed Internet Connection ✓ SecurID token and PIN ✓ Your Outlook/Entourage username and password for accessing E-mail and calendaring
	SNA ✓ A High-Speed Internet Connection ✓ SecurID token and PIN ✓ JavaScript enabled in your browser ✓ Cookies turned on in your browser ✓ Your HQ NT username and password for accessing your network files ✓ Your Outlook/Entourage username and password for accessing E-mail
Dial-in	✓ A NASA-issued laptop or registering home computer with NASA HQ Domain. (CICO 224 request) ✓ An analog phone line *Hint*: Most home phones and all fax lines are analog lines. ✓ SecurID token and PIN

2 Frequently Asked Questions (FAQs)

What if I want to remotely access HQ, but I did not bring home my Government-issued laptop?

Your home computer and Internet Service Provider (ISP) can be used to connect to NASA information technology resources. **Note:** Home computers must have antivirus software and IT security updates. Antivirus software is available from the NASA HQ Software Library by contacting the IT Help Desk at (202) 358-HELP (4357) or 1 (866) 462-7247. The Software Library will contact you when the software is ready for pick up. A software loan agreement outlining software use requirements must be signed. You must obtain the software prior to connecting remotely.

The following antivirus software is available for home use:

- Symantec AntiVirus 10 for Win XP only
- Symantec AntiVirus 8.1 for Win 2000
- Norton AntiVirus 10 for OSX (10.x)
- Norton AntiVirus 9 for OS 9
- Symantec Client Security 3.0.2 with STRONG Firewall—Beware!
- **Older versions of antivirus software are available upon request.

Note: HQ employees are not authorized to download any software, including shareware and freeware from the World Wide Web or other sources such as bulletin boards or install personal software on their office computers (including laptops). More information is available at:
http://www.hq.nasa.gov/office/codec/codeci/ITservices/help/software/swpol.htm#Service.

What should I do if I am unable to connect to information technology resources due to equipment malfunctions (computer, Internet connectivity, etc.)?

If you are unable to obtain a connection from your location, call the IT Help Desk at (202) 358-HELP (4357) or 1 (866) 462-7247.

Can I contact the IT Help Desk for support when working remotely?

The IT Help Desk can be contacted at (202) 358-HELP (4357) or 1 (866) 462-7247 to assist with Government-issued equipment and limited support related to connectivity issues from your home computer. **Note:** The IT Help Desk can not provide or change the password for your Domain account.

How do I get computer equipment, software, and supplies needed to perform my assigned duties?

Computer resources will be obtained using the current mechanisms (i.e., PCMall and ODIN Catalog). If these systems are unavailable, employees will be provided a Web site or e-mail address to submit requests for required resources. Employees will pick up their orders at a designated site. Disposal of computer resources will also be conducted at a designated site.

What if my computer equipment malfunctions or requires repair while I am off-site?

If your Government-issued equipment requires repair or malfunctions, call the IT Help Desk at (202) 358-HELP (4357) or 1 (866) 462-7247 and open a ticket. Bring the equipment to the designated site for repair as soon as possible. If you are at a COOP site, contact the on-site IT support. **Note:** A user is responsible for the repair of their personal equipment.

Can I forward my office telephone number to my off-site location?

A Voice Over IP (VoIP) telephone can be forwarded to any telephone. This can be done using the Call Forward All (CFwdALL) button on the VoIP telephone, or via the VoIP CallManager Web site. **Note:** This requires logging on to the Web site using the CallManager user ID and password provided during your VoIP telephone installation. This information must be obtained prior to working off-site.

How can I find information about emergency preparedness?

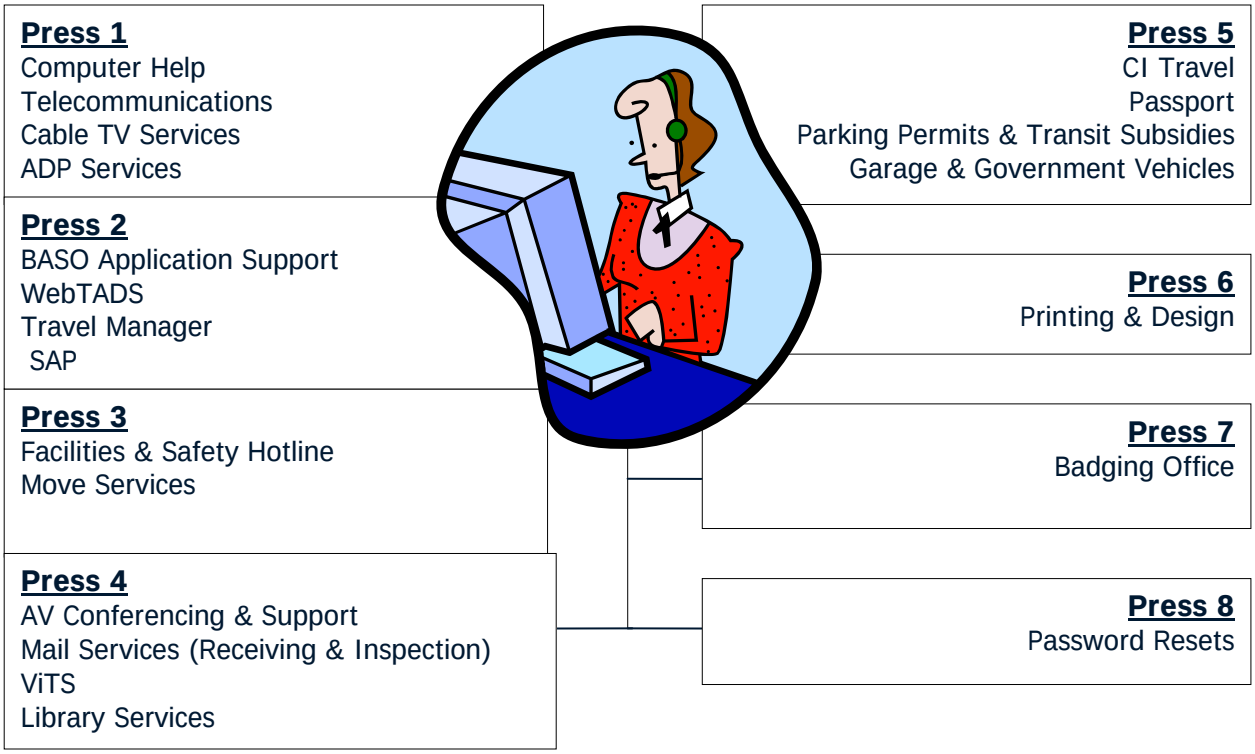
Your first stop for emergency communications is the Emergency Preparedness link found on Inside HQ. The Web site address is http://www.hq.nasa.gov/hq/emergency.htm. This Web site can be accessed prior to establishing a secure connection to NASA HQ.

3 Getting Help

The IT Help Desk provides IT support services at NASA HQ. The IT Help Desk staff is trained to assist users in resolving issues and concerns. If unable to resolve issues over the phone, the IT Help Desk will dispatch calls to the appropriate representative who will respond to, diagnose, or resolve the problem.

IT Help Desk services include desktop and laptop computers, administrative servers (i.e., file, print, e-mail, application, and internal Web servers), and remote dial-in capability. To request computer support, use the following methods: call the IT Help Desk at (202) 358-HELP (4357) or 1 (866) 462-7247, request e-support at https://www.odin.lmit.com/hq/helpdesk.html or send an e-mail message to service@hq.nasa.gov.

3.1 Phone Tree for (202) 358-HELP (4357)



3.2 Hours of Availability

At NASA HQ, desk-side technical support is provided between 6:00 a.m. and 6:00 p.m. Monday-Friday EST, except for holidays. After hours on-call support is provided for emergency requests and service for network systems, IT, heat, ventilation, and air conditioning/HVAC. Standard return to service time for desktop problems is 8 business hours, between 6:00 a.m. and 6:00 p.m. IT Support is available by telephone and e-mail 24x7 including weekends and holidays for status and problem ticket generation with limited support/problem resolution.

3.3 Getting Help Web Page

The **"Getting Help"** Web page is hosted by the HQ Information Technology and Communications Division (ITCD). This page offers information on the ITCD supported hardware and software as well as information on computer security, telecommunications, training and other related services.

Access **"Getting Help**" at http://www.hq.nasa.gov/itcd/get_help.html. It is also accessible through the ITCD home page at http://www.hq.nasa.gov/itcd/.

There are several other service help desks such as IEMP assistance, facilities support, and conference room scheduling. The IT Help Desk at (202) 358-HELP (4357) or 1 (866) 462-7247 will transfer the requester to the appropriate services if they are not the direct point-of-contact.

4 Web Sites to Bookmark

Bookmarking important Web sites allows a user to store and quickly access NASA Web sites from home.

- **OWA** - https://webmail.nasa.gov/ - Allows a user to access HEMI e-mail and calendar from any computer that is connected to the Internet. **Note:** The format for user logon is: hq\username.
- **Secure Nomadic Access** - https://sna.hq.nasa.gov/ - Allows the user to access NASA HQ shared folders and internal Web sites; a SecurID token is required. This will provide secure access from a home computer to NASA internal resources. **Note:** This Web site is not needed for Government-issued laptops that are configured with the NASA HQ VPN software.
- **Frequently Used Applications at HQ** - http://www.hq.nasa.gov/itcd/freq_used_apps.html - Provides links to frequently used NASA HQ applications.
- **Voice Over IP (VoIP) Telephones** - http://voip.hq.nasa.gov/ - Provides information on the Voice Over IP Telephones. This Web site is an added resource for answers to frequently asked questions and links to additional resource materials. It includes information about phone functionality.
- **CallManager** - https://nhqvpub01.voip.hq.nasa.gov/CCMUser/logon.asp - Provides access to the CallManager which allows set up of special VoIP features, including call forwarding.
- **Emergency Preparedness** - http://www.hq.nasa.gov/hq/emergency.htm - Can be accessed prior to establishing a secure connection to NASA HQ. Use this for emergency communications and to access the Emergency Preparedness links found on Inside HQ.
- **HQ ITCD** - http://www.hq.nasa.gov/itcd/get_help.html- Contains the ITCD supported hardware and software list. Also provides information about computer security, telecommunications, training and other related services
- **Facilities Help Desk System (FHDS) (NASA HQ Only)**
  https://polaris.hq.nasa.gov/FHDS/login.cfm
  FHDS allows NASA HQ users to submit and edit requests for facilities support services, Facilities Help Desk services or conference facilities services. In addition, it can be used to report HQ safety concerns.
- **Headquarters e-Directory (HQeD) (NASA HQ Only)**
  https://polaris.hq.nasa.gov/HQeD/search.cfm
  HQeD is the Web-based HQ phone book.
- **IT Help Desk**
  http://www.hq.nasa.gov/office/codec/codeci/ITservices/servctr/servdesk.htm
  The IT Help Desk can be used to submit a new ticket or check the status of an existing IT Help Desk ticket at NASA HQ.

- **PC Mall (Catalog)**
  http://www.pcmallgov.com/cap/login/
  NASA HQ catalog used to make software and hardware purchases.
- **SATERN (System for Administration, Training, and Education for NASA)**
  https://satern.nasa.gov/elms/learner/login.jsp
  SATERN is the Agency online Learning Management System (LMS) and an e-Training environment that supports the development of the NASA workforce through simplified and one-stop access to high quality training products and processes. Users can manage their learning plans, view and print their learning history, register for instructor-led and online courses, including internal and external training opportunities.
- **Travel Manager (NASA Only)**
  http://travel.hq.nasa.gov/
  NASA's automated travel authorization and travel voucher system.
- **USAJOBS**
  https://my.usajobs.opm.gov/login.asp?1=1
  This is a Federal employment site used by NASA employees. It provides tools to search and apply for jobs, create and submit resumes, and subscribe to job notification alerts.
- **WebTADS (NASA Only)**
  http://webtads.hq.nasa.gov/
  NASA system for employees to record work hours and labor charges.
- **X.500 Directory (NASA Only)**
  http://www.hq.nasa.gov/hq/x500/x500.html
  This is an electronic directory service that contains a listing of NASA employees and contractors.
- **Check In Check Out (CICO)**
  Access to CICO: http://www.hq.nasa.gov/itcd/cico.html
  This is a Web-based, automated workflow tool that will be used by HQ employees and contractors for submitting and processing work requests associated with a person's employment with NASA. Every HQ employee will be able to initiate requests for services in CICO, for themselves or another HQ employee.

5 IT User Workplace Responsibilities

- Fill out Forms 261 and 298 to obtain PKI software and certificates
- Follow the "Appropriate Use" Policy in the performance of your duties
- Maintain your own Directory record
- Back up your hard drive (C:) *
- Obtain annual IT security training
- Call IT Help Desk at (202) 358-HELP (4357) or 1 (866) 462-7247 for all IT services, problems, and other needs
- Consult with your IT Point-of-Contact (POC) for questions and requirements that can not be handled by the IT Help Desk

5.1 Maintaining the Security of Your Home Computer Is Your Responsibility

IT Security is a growing topic that applies to both work and home environments. Everyone with a computer and an Internet connection is at risk to a wide array of Internet threats. During the "Dial-Up Era", home systems were smaller targets for attackers because they were only sporadically connected to the Internet. With the emergence of home broadband (cable modem, DSL, wireless), users have more powerful connections and are connecting for much longer periods of time.

5.1.1 Threats

Threats include: Malicious Web Sites, Worms & Bots, Scammers/Phishers, Hackers, Unsecured Wireless Networks, Yourself

- ***Malicious Web Sites***

Malicious Web sites install software on computers that creates pop-up advertisements; hijacks Web sites, or contains viruses (Trojans, viruses, worms). They place tracking "cookies" on the computer to monitor browsing patterns. They exploit vulnerabilities in the browser to read, write, run, delete, or install files. Users obtain them through normal browsing, from an E-mail, or from links sent over an Instant Messenger client.

- ***Worms & Bots***

Infected machines attempt to break into a computer by exploiting vulnerabilities. They infect a computer with a worm or bot software to take control of the computer.

- ***Scammers/Phishers***

These are attempts to trick a user into giving up personal information, passwords, or money. Messages appear to be legitimate and are very convincing which makes it difficult for users to know it is a scam.

- ***Hackers***

Hackers pose similar threats as worms and bots. A hacker is a person attempting to break into your computer by exploiting vulnerabilities and cracking usernames and passwords. Hackers may be targeting you or the network you are on. They are assisted by bots and scanning tools.

- ***Unsecured Wireless Networks***

The default is no security! There is a backdoor into any network which allows anyone to connect to the Internet using your connection including neighbors, war drivers, or hackers.

- ***Yourself***

If a user makes system changes or opens files without knowing what they are doing puts them at risk. Disabling or not running important software to protect their systems and not keeping up-to-date with the latest patches and virus definitions are other ways to become vulnerable.

These threats can all lead to anything from annoying pop-ups, trouble accessing Web sites, loss of important files or data, theft of data and personal information. Identity attacks can be initiated against other systems and will appear to be coming from you.

5.1.2 The Defenses

- ***Being Aware!***

For many of these attacks, your judgment and actions are the first line of defense. Constantly be on the lookout for anything suspicious whether it is a Web site, E-mail, or Instant Message. If it smells fishy, then it probably is fishy. Do not blindly click links or agree to install programs unless absolutely sure they are safe. Never give out passwords to anyone, also be careful of where personal and banking information is entered.

- ***Strong Passwords***

Keep passwords secret and choose strong passwords. Use a mix of uppercase and lowercase letters with numbers and special characters (!, @, $, etc.). Make sure the password is at least 8 characters long. Do not use things that are easily known such as a name, address, phone number, or anything else that could be easily guessed.

  - **Good:** iTm2uA$p8, H_4dpZ$!s
  - **Bad:** Steven123, Nasa456

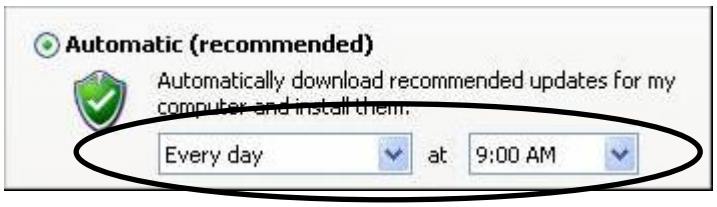
Use the first letter of a sentence plus a number and special characters that can be remembered. **Example:** the dog jumped over the yellow moon. Password could be: tDjotyM1%)

- ***Firewalls***

Many attacks from bots, worms, and hackers can be thwarted by a firewall. Never connect to the Internet without some form of a firewall. Firewall functionality is included in most, if not all, SOHO cable modems, routers, and wireless access points. Windows XP (SP2), Mac OS X, and most other Operating Systems come with firewalls built in. Third-party firewall products are easy to acquire and use (ZoneAlarm, Symantec).

- ***Installing Patches***

All vendor-recommended Operating System (Windows, Mac) patches should be installed. Both Windows XP and Mac OS X include a feature to automatically check for new updates. This can be found by going to start>Settings>Control Panel>Automatic Updates. Make selections from the drop-down menus to determine frequency of checking for updates.



With Windows XP Service Pack 2, the OS will download and install all recommended patches. Make sure the computer is configured this way.

Regardless of which OS is used, it should be configured to frequently check for new updates. Also, install patches for software that is used. If a message appears stating there are security updates, get them! (Browsers, MP3 Players, Firewalls, etc.)

- ***Antivirus software***

Most new PCs come with antivirus software. Buying the software is relatively inexpensive, and is worth the money (McAfee, Symantec). Most antivirus software contains features to protect against e-mail and Web-based viruses and Trojans, but this software should not be considered foolproof. Antivirus software should be configured to download new updates daily. Antivirus software is only as good as its signatures (definitions), make sure they are updated.

- ***Stopping Spyware***

Third-party products exist whose sole function is to find and eliminate spyware (Ad-Aware, Spybot S&D, etc). Some of the software runs constantly and stops new spyware before it can be installed. Many antivirus vendors are including anti-spyware technology in their products.

- ***Stopping Spam***

It is almost impossible to stop ALL spam, but there are things that can be done to reduce it. Most e-mail clients now come with spam filters that can be trained to stop almost 99% of all spam. Third-party products can be installed to provide additional protection. Most e-mail providers, such as Hotmail and Yahoo, provide spam filtering as part of their free and paid e-mail services. Have a secondary e-mail account for signing up for things on the Internet.

- ***User Accounts***

Make sure "Guest" accounts are disabled or deleted (not possible in Windows). Make sure all of your accounts have passwords and that they meet the criteria previously mentioned for a strong password. Delete or disable any accounts you are not using anymore (i.e. if your friend or family had an account they are no longer using).

- ***Data Backup***

Frequently back up your data including e-mail, financial documentation, and other important documents or files on the hard drive. Back up all important data to a CD, DVD, or flash drive. Periodically store a copy of this data off-site in a secure location.

- ***Wireless network security***

Most wireless access points are not secure by default. Change the default Service Set Identifier (SSID) to something easy to remember but secure enough that someone can not guess it. **Example:** Last name mixed with numbers (double91eagle64). The SSID does not provide any data-privacy functions. Disable broadcast of the SSID. At a minimum, use 128-bit WEP encryption, with a randomly generated hexadecimal key. The preferred security method is WPA or WPA2 with a secure authentication password. Most wireless access points support all of these security options, and offer relatively easy-to-use interfaces for configuration.

- **Security Updates:**
  - http://www.microsoft.com/security/default.mspx for Microsoft Security Updates
  - http://docs.info.apple.com/article.html?artnum=61798 for Apple Security Updates
- **Software Downloads:**
  - http://zonelabs.com for ZoneAlarm Firewall

- http://www.clamav.net for Clam AntiVirus
- http://www.lavasoftusa.com for Ad-Aware Personal Edition spyware protection
- http://www.safer-networking.org for Spybot Search & Destroy
- http://www.microsoft.com/athome/security/spyware/software/default.mspx for Microsoft's anti-spyware protection
- http://toolbar.google.com for the Google toolbar to stop pop-ups (for IE)

- **Definitions & Information:**
  - http://nonadmin.editme.com/WhyNonAdmin for details on why not to run your machine as an Administrator and what steps you can take to protect yourself
  - http://en.wikipedia.org/wiki/Main_Page for the online Open-Source multilingual encyclopedia
  - http://www.webopedia.com for a great resource for computer and technology definitions
  - http://www.howstuffworks.com is a great Web site on how all kinds of things work. There is a lot of information on home networking, computers, and technology in general

- **Keeping safe:**
  - http://www.ftc.gov/bcp/edu/pubs/consumer/alerts/alt127.shtm - FTC consumer alert for: How Not to Get Hooked by a 'Phishing' Scam
  - http://www.consumer.gov/idtheft - FTC Web site for spotting, protecting, and defending against identity theft

5.2 Securing Sensitive Information at NASA HQ

To ensure that federal agencies are protecting sensitive information, on May 22, 2006, the Office of Management and Budget (OMB) issued a memo (M-06-15) to all government agencies regarding the safeguarding of personally identifiable information. Deputy Administrator Shana Dale reminded NASA employees of their special duty to protect privacy information in a message dated June 9, 2006. On June 23, 2006, OMB issued another memo (M-06-16) to all government agencies regarding the need to protect sensitive agency information.

Accordingly, data encryption software is being deployed to all NASA HQ desktop and laptop computers as an initial step in improving the protection of sensitive information. This provides the ability to encrypt information prior to transmission or storage and to decrypt information upon receipt. HQ will offer briefings and training for all employees to provide insight on identifying and safeguarding sensitive information, the NASA and federal policies, and penalties for the mishandling or wrongful disclosure of sensitive information.

- **Personally Identifiable Information (PII)**

PII is described by OMB as information about an individual maintained by an agency, including education, financial transactions, medical, criminal, or employment history. It also includes information which can be used to distinguish or trace an individual's identity, such as name, social security number, date and place of birth, mother's maiden name or biometric records.

We all have the responsibility to ensure the protection of sensitive information by applying appropriate safeguards. This applies to information stored and/or processed on computer systems, hand held devices, removable media of any kind, and any format including graphic

images and printed documents. Individuals who are authorized to remotely access, collect or process sensitive information and those who telecommute will need to be especially vigilant in safeguarding and protecting this information.

All Windows users are required to use Entrust ICE to encrypt data files. If you are not currently an Entrust user, please complete NHQ Form 261, Application for Digital Certificate, to request the Entrust software and a digital certificate. Windows users are not required to fill out Form 298. All Macintosh users are required to complete NHQ Form 261 and NHQ Form 298, NASA Public Key Infrastructure (PKI) Agreement for PKCS-12 Export.

If you are unable to attend a training session, Forms 261 and 298 can be obtained from the NASA Forms Web site at https://pollux.hq.nasa.gov/nef/user/form_search.cfm

Follow the site instructions for form submission to the Information Technology and Communications Division (ITCD). Training is available. Training focuses on NASA and federal policies in addition to the penalties for the mishandling or wrongful disclosure of sensitive information.

Contact the HQ Computer Training Center (http://ctc.hq.nasa.gov) at (202) 358-1111 or ctc@hq.nasa.gov for more information. See the following Web site for additional information: http://www.hq.nasa.gov/office/codec/codeci/pki/cert.htm

To read the full text of the previous IT Notice on Securing Sensitive Information at NASA HQ, dated October 10, 2006, please visit:
http://www.hq.nasa.gov/office/codec/codeci/whatsnew/fy2006/11010601.htm

For questions relating to the Privacy Act and/or Personally Identifiable Information (PII), please contact the HQ Privacy Act Manager, Bryan D. McCall, at (202) 358-1767.
For more information relating to current NASA Privacy Policy, see NPD 1382.17G, at:
http://nodis3.gsfc.nasa.gov/displayDir.cfm?Internal_ID=N_PD_1382_017G_&ppage_name=main

For questions relating to encryption software and functions, please contact the IT Help Desk at (202) 358-HELP (4357) or 1 (866) 462-7247.

- **Administratively Controlled Information (ACI)**

Administratively Controlled Information (ACI) is sensitive, but unclassified, information that is not national security information but must be protected from disclosure. It must be properly marked and locked up when not under the supervision of the authorized personnel and must be encrypted when transmitted over a non-secure network. Examples include: trade secrets, proprietary information, Freedom of Information Act exempt information, financial information, and personnel records.

- **Scientific & Technical Information (STI)**

Scientific & Technical Information (STI) are results of basic and applied scientific, technical and related engineering research and development. It includes the management, industrial and economic information relevant to this research. Examples include: technical papers and reports, journal articles, papers and presentations for meetings and conferences, and non-published in-progress reports or documents in internal repositories that will not be released outside of NASA.

- **International Traffic in Arms Regulation/Export Administration Regulation (ITAR/EAR)**

International Traffic in Arms Regulation/Export Administration Regulation (ITAR/EAR) deals with restrictions on the export of articles and services including information and technical data about those items. There are significant legal consequences for not obeying these laws.

- **Encryption**

Entrust

Entrust is currently not permitted to be installed on home systems due to licensing, performance, configuration, and support issues. Use of Agency sensitive and PII data on personally-owned computers is not advocated nor supported by NASA. This is per Agency direction and Center policy (OCIO & Privacy Manager). The only approved use of Entrust on multiple systems is if they are NASA-issued computers.

IMPORTANT: E-mail encrypted at work can not be read from your home computer using Outlook Web Access—unless it is a NASA-issued computer and you are using the full Outlook client for e-mail, and the Entrust software and certificates are installed on that computer. Even when not connected to the HQ network or the Internet, Entrust can still be used to work offline and encrypt/decrypt documents.

The full Entrust PKI User Guide for Macintosh and PCs is available online. For more information about obtaining Entrust on NASA-issued computers, including laptops, or to obtain the Entrust PKI User Guide, please visit the NASA HQ PKI Entrust Home Page at http://www.hq.nasa.gov/itcd/itsecurity/pki_entrust.html

Public Key Infrastructure (PKI)

The Public Key Infrastructure (PKI) is a combination of software, encryption technologies, and services that enables enterprises to protect the security of their communications and business transactions on the Internet. Entrust is the software NASA has selected as its PKI software. Entrust is supported on both Macintosh and PC computers.

PKI uses two encryption keys and two signing keys. The public set is stored with your certificate in the X.500 Directory; the private set is stored with your Entrust profile on the hard drive.

When the recipient receives your signed and encrypted message, the private keys are matched to the public keys on the certificate. This enables the recipient to decrypt the message and verify your identity.

When sending an encrypted e-mail message containing sensitive or PII data, you should also include a digital signature. This provides three levels of protection that are distinct from the kind of protection you get from encrypting:

- **Integrit**y: Digitally signing a message ensures the message and its attachments have not been modified since it was signed.
- **Authentication:** It verifies the identity of the originator of the message.
- **Non-repudiation:** A digital signature guarantees that it can verify who the sender and the recipient were.

Requesting an Entrust Certificate

You must request a digital certificate in order to use Entrust. This is done by completing an NHQ 261 form and having it approved by your supervisor. Contractor employees must also obtain the approval of their Contracting Officer Technical Representative (COTR). All requests must be signed and dated by the requester. Macintosh computer users must also complete an NHQ 298 form. Completed and approved forms must be delivered to Room 4A35. They should then be date stamped and entered into the Incoming Forms Log in the Other Forms section. The assigned Request Number should be written in the upper right hand corner of the NHQ 261 and NHQ 298 (Macintosh users only).

To process the request, your identity must be positively verified. This is done as part of a background investigation when you are hired. The Registration Authority (RA) will check with the HQ Security Office to see if the background investigation is complete. If it has, your form will be forwarded to account administration to create the certificate. This process will take approximately two or three working days. If the investigation is not complete, you will be sent an e-mail asking you bring two of the following four approved forms of identification to the RA:

- Drivers License or State Issued Identification Card
- Birth Certificate
- U.S. Passport
- U.S. Naturalization Papers

New Hires whose background investigation is still pending, can avoid delays by bringing two forms of identification, along with the NHQ 261 and NHQ 298 (Macintosh users only) forms, to the NHQ RA in Room 4B37.

Upon approval, the certificate request will be sent to Account Administration for processing. They create the certificate and a ticket to get the Entrust software installed on your workstation. You will be notified by e-mail or phone when the certificate is ready. You will be given information on where to pick up the certificate activation codes. Account administration has up to three working days to create a certificate once they receive a request.

Questions on the status of certificate requests should be directed to Account Administration at (202) 358-0451 or (202) 358-2188.

Forgotten Passwords

The Entrust password is the key required to utilize the certificate for encryption/decryption and digital signing of documents or messages. If you forget the password, a NHQ 262 form must be submitted to have a new one issued. All requests must be signed and dated by the requester. Approved forms must be delivered to Room 4A35, where they should be date stamped and entered into the “Incoming Forms Log” in the Other Forms section. The assigned Request Number should be written in the upper right hand corner of the NHQ 262 form. Requests will be processed within three working days.

Pretty Good Privacy (PGP)

PGP is an accepted solution for encrypting/digitally signing e-mail for use in communications with those in private industry, education, or other federal agencies that do not use PKI. Although PGP is not the Agency standard, it is supported for those specific uses on NASA-

issued systems because an item encrypted with PKI can not be decrypted with PGP and vice-versa. PGP can be used on home systems if purchased by the user. Support for home use is limited.

E-mail Practices

- Handling Spam, Offensive, or Threatening E-mail
- Report offensive or threatening e-mail to abuse@hq.nasa.gov.

Spam Filter

All incoming e-mail passes through the Spam Firewall before entering NASA HQ e-mail systems. Based on policy settings, the Spam Firewall:

- allows the e-mail to pass through
- deletes the e-mail, or
- quarantines the e-mail

Incoming mail with any of the following characteristics is deleted:

- contains a known virus
- contains file attachments with known Microsoft OS executable file extensions
- is sent from an Internet domain whose sole intent is known to be the generation of unsolicited junk e-mail

Incoming mail that has a high probability of being unsolicited junk mail is quarantined:

- This prevents mail from cluttering up your e-mail in-box or handheld device.
- You will receive regular e-mail notifications about your e-mail being held in the quarantine, and you will be able to retrieve or delete these messages yourself.

You can "train" the Spam Firewall when it makes a mistake:

- specify Internet addresses or domain names that should always be able to send you mail ("whitelist")
- specify Internet addresses or domain names that should never be able to send you mail ("blacklist")

5.3 Security Concerns: Computer Incidents

- **Annual IT Security Awareness Training**
  - All NASA employees must complete IT Security Awareness Training annually.
  - New employee orientation DOES NOT satisfy the annual requirement.
  - Training is offered via the NASA SATERN Learning Management System (https://satern.nasa.gov) or classroom sessions at HQ.
  - See the **"Training & Awareness"** page at http://www.hq.nasa.gov/itcd/itsecurity/it-security.html for completion deadlines, classroom training schedules, and more information.

- **Password Procedures**
  - Must be at least 8 characters long
  - Must contain at least one alpha, one numeric, and one special character

- Must not contain any form of your name, user ID, birth date, family member name, personal information, dictionary words, NASA project or Organization name, vendor product, sports team names, vehicle names, etc.
- If you must write it down, LOCK IT UP!
- Don't wait until it expires to change it

5.4 How to Change Your HQ Domain Password

5.4.1 For PC Users at HQ

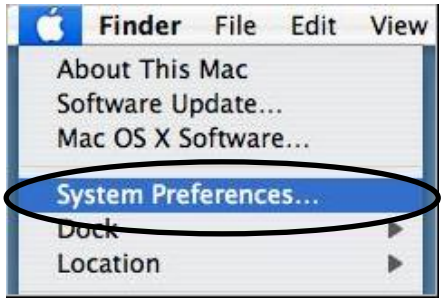
1. Press **Ctrl+Alt+Delete** on the keyboard.
2. The **"Windows Security"** window will open, click "**Change Password"**.

3. Enter the current password in the **"Old Password:"** field.
4. Enter the new password in the **"New Password:"** field.
5. Confirm the new password by entering it in the **"Confirm New Password:"** field, and click "**OK"**.

5.4.2 For Macintosh OS X Users at HQ

1. Click on the blue **APPLE** in the upper left corner of your screen.

2. Select "**System Preferences"** from the menu.

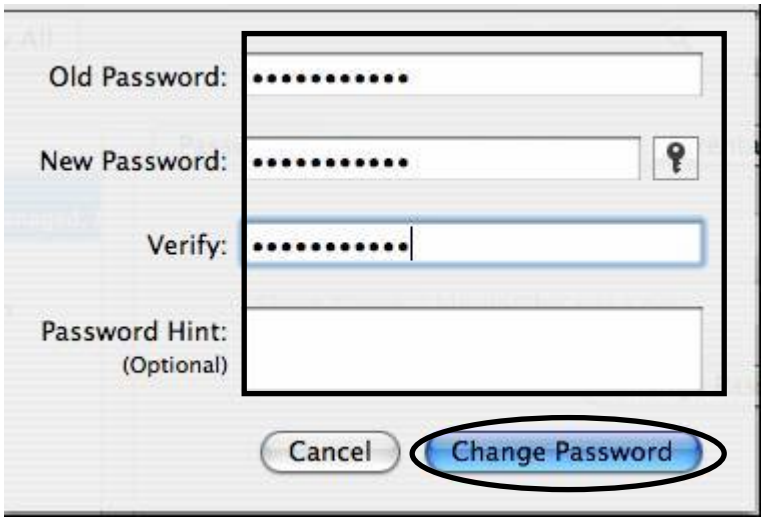


3. In the System Preferences window, click on "**Accounts"**.

4. In the Accounts window, select your user ID from the list on the left.
5. Click the "**Change Password…"** button. (Open the yellow lock at the bottom left-hand side of the Accounts window, if necessary.)

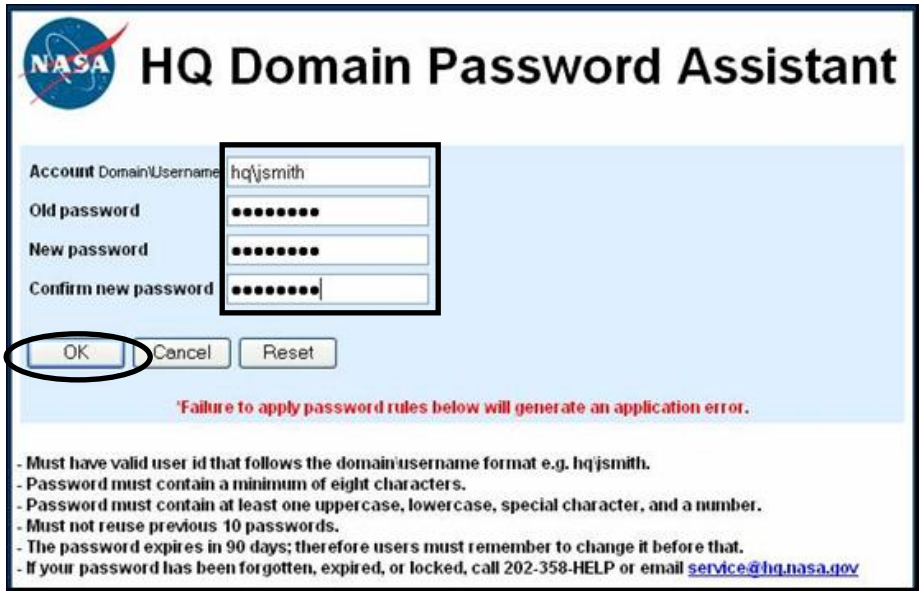
6. Enter the current password in the **"Old Password:"** field.
7. Enter the new password in the **"New Password:"** field.
8. Enter the new password again in the **"Verify:"** field.
9. Click **"Change Password"**.

Note: A password hint can be entered in the **"Password Hint:"** field.



5.4.3 For Remote Users (PC or Mac)

1. **Connect to HQ** via HQ Dial-In, SNA, or VPN.
2. Go to https://nasasupport.hq.nasa.gov/aexp2.asp. (Mac users must use the Safari browser.)
3. Enter your (HQ) **domain username**, **current password**, and **new password** twice in the appropriate fields.
4. Click "**OK"** to change your password.
5. Click "**Cancel"** to cancel the password change.
6. Click "**Reset"** to clear the form and start over.



5.5 Frequently Asked Questions

What are the HQ domain password requirements?

Your new password must comply with the following requirements:

- The password must have a minimum of eight characters
- The password must contain at least one character from at least three of the four following sets of characters:
  - Uppercase letters (A, B, C, etc.)
  - Lowercase letters (a, b, c, etc.),
  - Special characters (~, !, @, #, $, etc.)
  - Numbers (1, 2, 3, etc.)
  - You may not reuse any of your previous 10 passwords

It is important to remember that the password you use is case-sensitive, meaning that the system recognizes the difference between an uppercase "A" and a lowercase "a".

Who do I call if I have trouble changing my workstation password?

If your password has been forgotten, expired, or locked, or if you can not complete the password reset process, call IT Help Desk at (202) 358-HELP (4357) or 1 (866) 462-7247.

Why am I being asked to change my workstation password?

To maintain compliance with NPR 2810.1, all NASA computer users must periodically change their passwords. The NASA Procedural Requirements (NPR) 2810.1 provides guidance and requirements for account password complexity.

How often will I be asked to change my workstation password?

For the NASA IT resources accessed through your HQ domain password, the password lifetime is 90 days. New passwords will automatically expire in 90 days.

You will be asked to change your password every 90 days and will receive notification via e-mail to do so. Failure to change the password by the due date will result in the account being disabled; only a call to the IT Help Desk at (202) 358-HELP (4357) or 1 (866) 462-7247 will reset the account and enforce the new complex password after it has been disabled.

How can I create a strong password?

- Use at least one symbol or number (preferably not just one at the end or at the beginning).
- Use a varying combination of lower- and upper-case letters (for example: IsDlMs).
- Use more than eight letters or symbols; hackers try short words first.
- Use two words that normally don't go together that are separated by a punctuation mark or number.

For example, s+@r3laTer! (meaning "starblaster") would be difficult to guess.

- Use the first letters of a phrase you can remember with numbers and special characters.

For example, "I sure do love my spouse number 1!" becomes the difficult-to-crack (Isdlms#1!).

- The intent is to create passwords that are not only not easy to guess, but are also difficult to "crack" using hacker software tools.

Passwords should not be created from an easily guessed word such as your name, user ID, employee ID, or any variation thereof (backwards, changing case, etc.), or be coined from any

word referring to anything personal about you, such as the name of your spouse, child, pet, favorite football team, or literary character.

What more can I do to keep my new password secure from hackers and others?

- Properly protect password records. If you must keep a record of your passwords, seal the list in an envelope and place it in a locked desk drawer or overhead bin. Do not record them on sticky notes on walls, monitors, or under keyboards. Do not write them down in your Rolodex or your calendar. These are the first places people will look if they are trying to steal your password.
- Never share your password with others. Your passwords are for your use only. This includes trusted co-workers, family members, and your manager. There are ways to share information, calendars, and e-mail without disclosing your passwords. Contact your IT POC or the IT Help Desk at (202) 358-HELP (4357) or 1 (866) 462-7247 for more information.
- Avoid typing your password when another person is looking over your shoulder or otherwise watching you type.
- Change your passwords regularly. Our systems are designed to enforce a password change every 90 days. Don't wait until you have to change your password. If you believe your password might have been compromised, change it immediately!

5.6 Appropriate Use of IT Resources

NASA IT Resources are for OFFICIAL BUSINESS and other authorized activities; limited personal use is permitted, provided:

- It does not interfere with NASA missions or operations
- It does not affect employee productivity
- It does not incur additional expense to the Government
- It does not violate the Standards of Ethical Conduct for Employees of the Executive Branch (5 CFR 2635)

5.7 IT Prohibited Practices

- Outside fund-raising, endorsement, lobbying, or participation in prohibited partisan political activity
- Creation, downloading, viewing, storage, copying, or transmission of sexually explicit material or materials related to gambling, illegal weapons, terrorist activity, or controlled substances
- Circumventing or disabling IT Security measures such as antivirus software or attempting to deprive authorized users access to a resource
- Illegal or unauthorized entry into or modification, destruction, manipulation, or denial of access to information residing on ANY information system
- Use of a NASA computer system in any way that might be interpreted as an attempt to influence a member of Congress regarding legislation or appropriation
- Loading software or moves, additions, alterations, or replacement of any HQ computers, network connections cable plant, or other IT resources without express permission of HQ CIO
- Unauthorized acquisition, use, reproduction, transmission, or distribution of any controlled information that includes privacy act, copyrighted, trade marked, or material with other intellectual property rights; proprietary data; or export controlled information

Downloading Software:

- Do not disable software on your computer
- Do not load (or download) software or Windows patches; it can causes a serious breach of security
- Results in a $150 charge for a restore to service

5.8 What is a Virus?

Viruses are one of the major threats that systems and information everywhere encounter. Practically every day there is mention of a new virus that is designed to inconvenience users or cause damage. A virus is a program or code that replicates itself onto other files. A virus can infect another program, boot sector, partition sector, or a document that supports macros by inserting or attaching itself to that medium. Most viruses have the capability of replicating themselves. Additionally, many can do a variety of damage to a computer system including deleting or altering files, sending e-mail, etc.

Worms are programs that infect and propagate themselves through various transport mechanism such as file copies, e-mail, etc. Worms may do damage and compromise the security of the computer. They can arrive in a system through various means, but are most commonly acquired through exploitation of system vulnerabilities or by clicking on an infected e-mail.

Trojan horses disguise themselves as something other than what they appear to be at the point of execution. Trojan horses generally do not copy themselves; rather they must be sent by someone or carried by another program. They frequently are embedded in a joke program or other attractive software. The type of damage caused by Trojan horses may be anything undesirable for a computer user. The most popular includes data destruction or compromising a system by providing a means for another computer to gain unauthorized access.
Symantec's Virus Encyclopedia
http://www.symantec.com/enterprise/security_response/threatexplorer/threats.jsp

Hoaxes generally contain a message of great urgency, warning about some type of destructive virus that spreads quickly, causing extreme damage. The hoax creator's goal is to cause panic among users. There are two known factors that are essential to a successful virus hoax. They are: (1) technical sounding language, and (2) credibility by association. A clue that it might be a hoax is if the warning urges you to pass it on to your friends. Being concerned individuals, many will distribute the hoax. DO NOT circulate virus warnings without first checking with the IT Help Desk at (202) 358-HELP (4357) or 1 (866) 462-7247 or the IT Security Team (202) 651-8505.

For more information about hoaxes, please visit one of the following Web sites:
"DOE Computer Industry Advisory Capability Hoaxbusters" http://hoaxbusters.ciac.org/
"Symantec's Virus Hoaxes"
http://www.symantec.com/enterprise/security_response/threatexplorer/risks/hoaxes.jsp

Contact the IT Help Desk at (202) 358-HELP (4357) or 1 (866) 462-7247 to report viruses and hoaxes, or to request assistance.

5.8.1 Virus Products and Information

All HQ-issued workstations and laptops are equipped with antivirus software as part of the standard workstation core load. Antivirus software updates are released on a regular basis. It is essential for users to keep their antivirus software up-to-date. All users are requested to shutdown and reboot their workstation sometime during each workday. When a workstation is booted, it will check for and load the latest antivirus software updates. Laptop users should connect to the HQ Private Network regularly to ensure they receive updates. Laptop users who will be on the road should contact the IT Help Desk at (202) 358-HELP (4357) or 1 (866) 462-7247 to find out how to receive updates remotely.

The desktop virus protection products used at NASA HQ are also available to HQ Civil Servants for use on home computers. Contact the IT Help Desk at (202) 358-HELP (4357) or 1 (866) 462-7247 to request a copy.

5.8.2 Virus Response

If you suspect your computer is infected with a virus, please report it immediately to the NASA IT Support Center via one of the mechanisms listed below.

NASA IT Support Center Online Ticket Submission Web Site:
https://www.odin.lmit.com/hq/helpdesk.html
You will be required to fill in certain text blanks; enter as much detail as possible.

To report a virus via telephone, please call the NASA IT Support Center at:

- (202) 358-HELP (4357) from within NASA HQ
- 1-866-4NASAHQ (462-7247) domestic and international toll-free, where available

Note: If the response is unsatisfactory, it is recommended that customers contact the following HQ Information Technology and Communications Division personnel:

- Gregory Kerr (202) 358-2218
- Andy Boncek (202) 358-7218
- Scott Oglesby (202) 358-0654

5.8.3 Antivirus Software

Antivirus software is available to you from the NASA HQ Software Library. In order to request this software, you must contact the IT Help Desk at (202) 358-HELP (4357) or 1 (866) 462-7247. A ticket will be generated for you. The Software Library will contact you when your software is ready for pick up. You will be asked to sign a software loan agreement outlining software use requirements.

The following antivirus software is available for home use:

- Symantec AntiVirus 10 for Win XP only
- Symantec AntiVirus 8.1 for Win 2000
- Norton AntiVirus 10 for OSX (10.x)
- Norton AntiVirus 9 for OS 9
- Symantec Client Security 3.0.2 with STRONG Firewall—Beware!

***Older versions of MS Office and antivirus software are available upon request.*

6 VoIP Phone

Voice mail services on HQ telephones include: standard voice mailboxes, special menu boxes, FAX store-and-forward boxes, and integration of mail boxes and pagers. Small orders for initial service, changes, and problems can be called in to the IT Help Desk at (202) 358-HELP (4357) or 1 (866) 462-7247.

6.1 Accessing Your Voice Mail Account

There are two methods to access the VoIP phone voice mail:

- Call (202) 358-HQVM (4786) or toll-free 1 (866) 358-HQVM (4786)
- Call your office phone number and press the * key after voice mail starts
  1. Enter your ID (this is the last 4 digits of your HQ phone number)
  2. Press the pound (#) key
  3. Enter your password
  4. Press the pound (#) key
- **VOICE MAILBOX MENU OPTIONS**

  Press 1 – Review Messages
  Press 2 – Send a Message
  Press 3 – Review Old Messages
  Press 4 – Setup Options
- **SETUP OPTIONS MENU**

  Press 1 – Change Greetings
  Press 2 – Message Settings
  Press 3 – Personal Settings
  Press 4 – Transfer Settings
  Press 0 – Help
  Press * – Exit

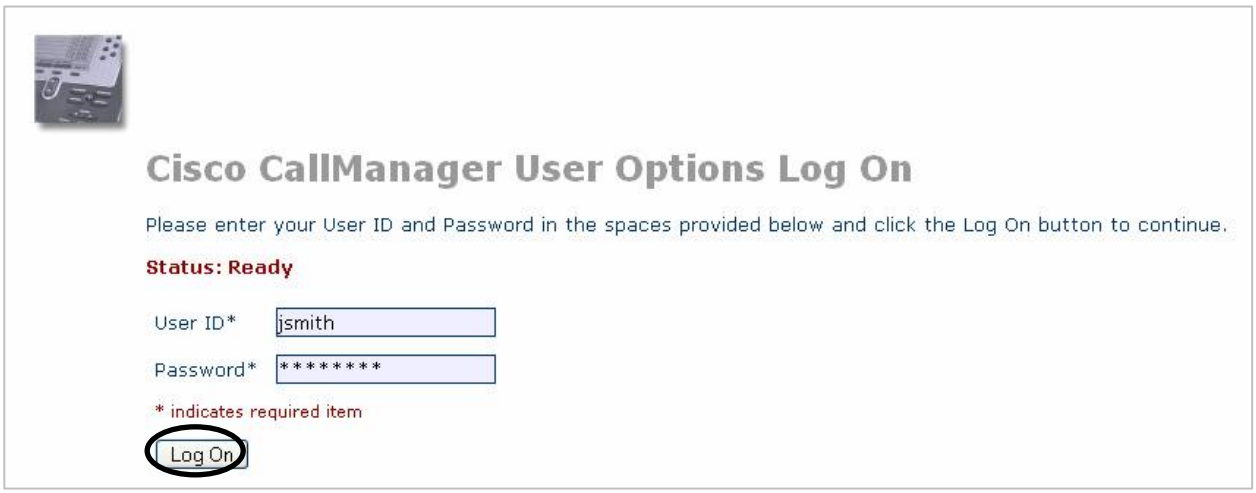
6.2 Activating the Call Forward Feature

1. From the **"Cisco CallManager"** (CCM) Web site, click the link to log on. http://voip.hq.nasa.gov/

2. The **"Security Alert"** dialog box will display, click **"Yes"** to accept the certificate.

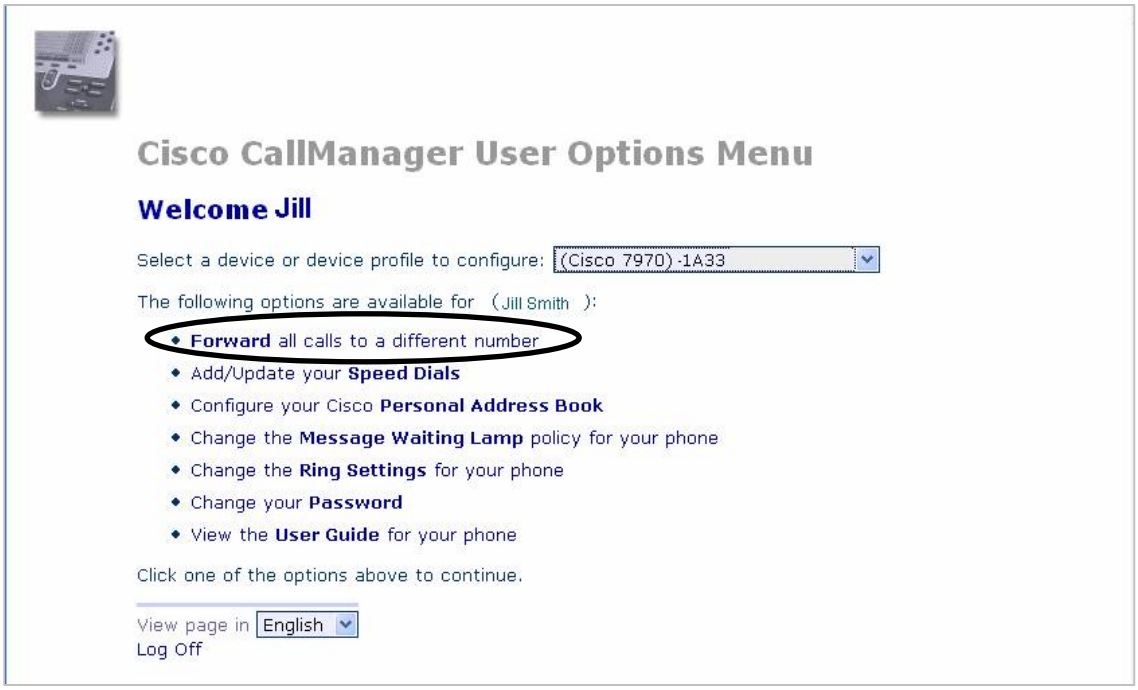
3. Enter your HQ domain username in the **"User ID*"** field and the password issued to you when you received your VoIP phone. It is located on the back of the VoIP tri-fold.

Note: The password requested is your CCM password, not the voice mail password. If the CCM password is unknown, contact the IT Help Desk at (202) 358-HELP (4357) or 1 (866) 462-7247.

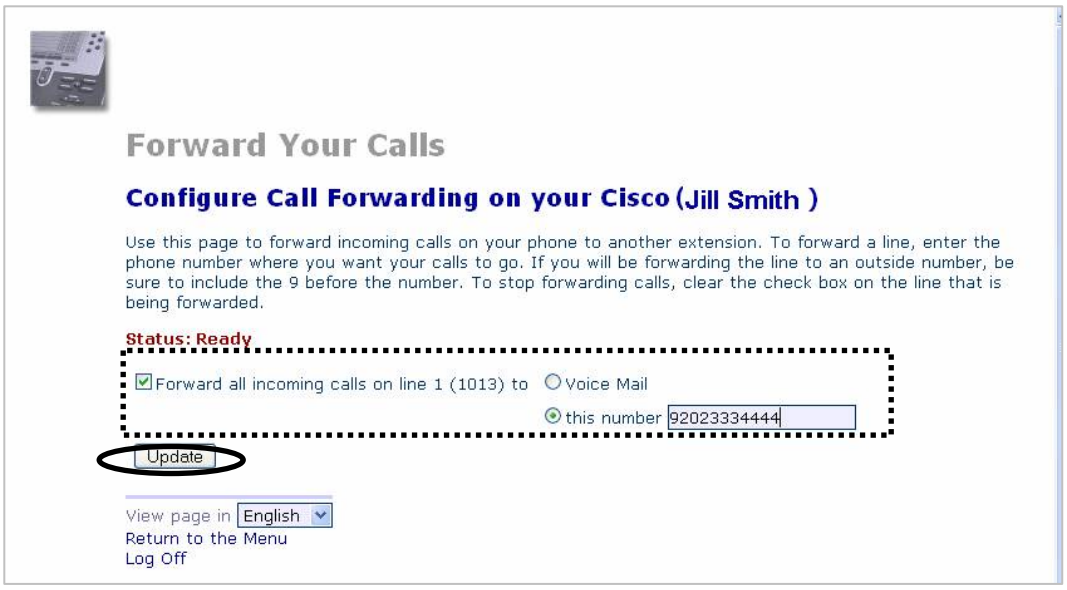


4. Click **"Log On"**.

The **"Cisco CallManager User Options Menu**" will display; click on "**Forward all calls to a different number"**.



5. The **"Forward Your Calls**" window will display; click the checkbox to forward incoming calls.



6. Select the radio button for forwarding calls to voice mail or to another number.
7. To forward to *another number*, **type the number** in the text box to the right.
8. To forward to an *outside number*, **type 9 and the number**.
9. If forwarding to a *long distance number*, **type 91 the area code and number**.
10. Click "**Update"**.

Note: Spaces, dashes, or other characters should NOT be included in the forwarding number.

11. A message will display stating **"Status: Update completed successfully…"**.

- **From the VoIP Phone**

  1. Press **CFwdAll** located on the soft keys. (You will hear a special dial tone.)
  2. Enter the number you would like to forward your calls to (for an *outside number*, **you must enter 9** and then the number; for *long distance*, **you must enter 91** then the area code and number).
  3. To forward to voice mail, Press "**CFwdAll"** and **dial 4786** or press "**CFwdAll"** and press the "**messages"** button.
  4. When complete, the forwarded number appears at the bottom of the screen.

6.3 To Deactivate Call Forwarding

- **From the VoIP Phone**

  1. Press **CFwdAll** located on the soft keys; you will hear a beep indicating that the forwarding has been removed.

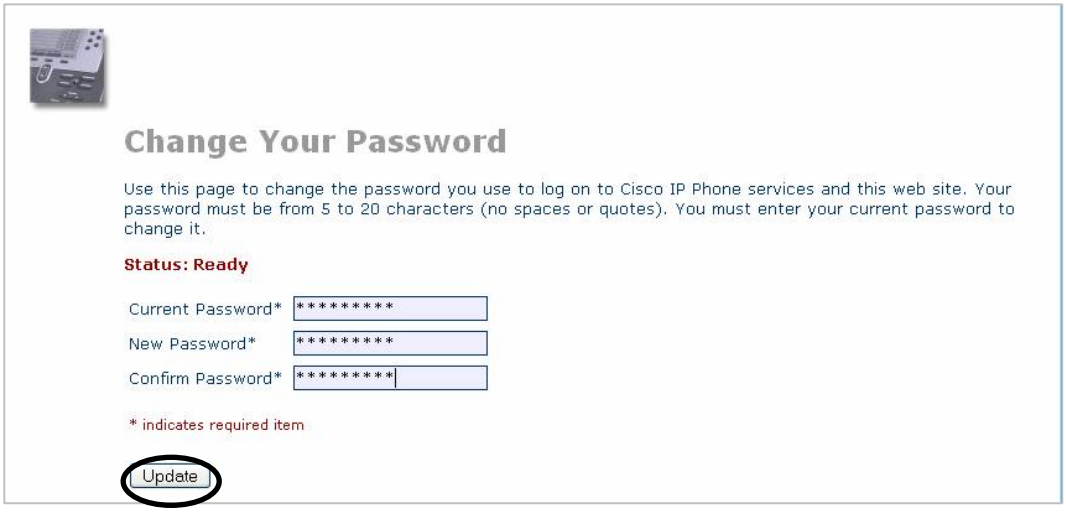
- **From the Web**

  1. Log onto the CCM Web site: http://voip.hq.nasa.gov/
  2. Click on **"Forward all calls to a different number";** uncheck the checkbox for **"Forward All Calls"**.
  3. Click "**Update**".
  4. A message will display stating **"Status: Update completed successfully…"**.

6.4 How to Change Your CallManager Password

1. From the **"Cisco CallManager User Options Menu"**, select **"Change your Password"**.

2. The **"Change Your Password"** window will open; enter your current password in the **"Current Password*"** field.
3. Enter your new password in the **"New Password*"** and **"Confirm Password*"** fields.
4. Click, **"Update"**.



5. A message will display **"Status: Update completed successfully; use your new password next time you log on"**.

7 Accessing HQ IT Services

This section provides instruction for network connection and how to access HQ IT Services.

7.1 Internet Connection Using a Home Computer

The various methods of connecting to the Internet from a home computer are outside the bounds of this document. Contact your Internet Service Provider (ISP) to determine the best way to connect or troubleshoot a network connection.

7.2 Internet Connection Using a NASA-Issued Laptop

Note: A user can send and receive e-mail using Microsoft Outlook on a NASA-issued laptop. Neither VPN nor SNA are required to use the full-featured Microsoft Outlook.

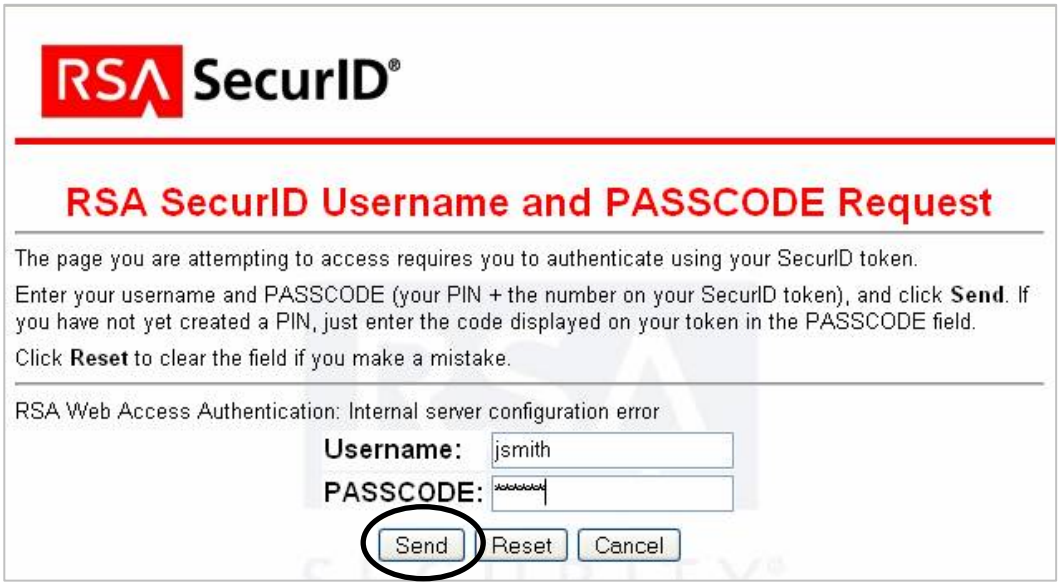
1. Locate the Ethernet cable that was provided when the laptop was issued. It may be located in the carrying case that came with the laptop. It can be blue or yellow; color does not matter. An Ethernet Cable (RJ-45) looks like a standard telephone cable (RJ-11), except wider. This illustration shows the end of an Ethernet cable.

2. Connect the Ethernet cable to one of the Ethernet ports on the rear panel of the laptop, as shown in this illustration.

3. Connect the other end to the matching slot on the back of the external modem. When properly connected, the Ethernet cable will be locked into place and can only be removed by pressing the plastic tab located on the connector while pulling the cable out. **Note:** Regardless of the Internet connection method, in some cases you may need to reboot your external modem.

7.3 SecurID Token - Resetting the PIN

1. Open a Web browser and go to https://pollux.hq.nasa.gov/securid .
2. Enter your user ID in the **"Username:"** field. For example: jsmith (Use the first initial of your first name and up to the first seven letters of your last name.)
3. Enter the current SecurID 6-digit number displayed on the token in the **"PASSCODE:"** field.



4. Click **"Send"** (DO NOT PUSH ENTER ON YOUR KEYBOARD).
5. Create a new pin containing 4 to 8 digits.
6. Enter the new pin in both the **"New PIN:"** and **"Verify New PIN:"** fields.
7. The pin can be all numbers, all letters, or a combination of numbers and letters. No special characters are permitted (i.e. * ! # @ % $&^?).

8. Click **"Send"**. (DO NOT PUSH ENTER ON YOUR KEYBOARD).

9. Your PIN has been successfully set.
10. The next screen is the verification screen.
11. Enter your username and your newly created pin plus the 6-digits appearing on your token. **Note:** Always wait for the next set of 6-digit numbers to change before entering.
12. Click **"Send"**. You should get a message stating that if you have reached this page you have successfully initialized your pin. Your token is ready to be used.

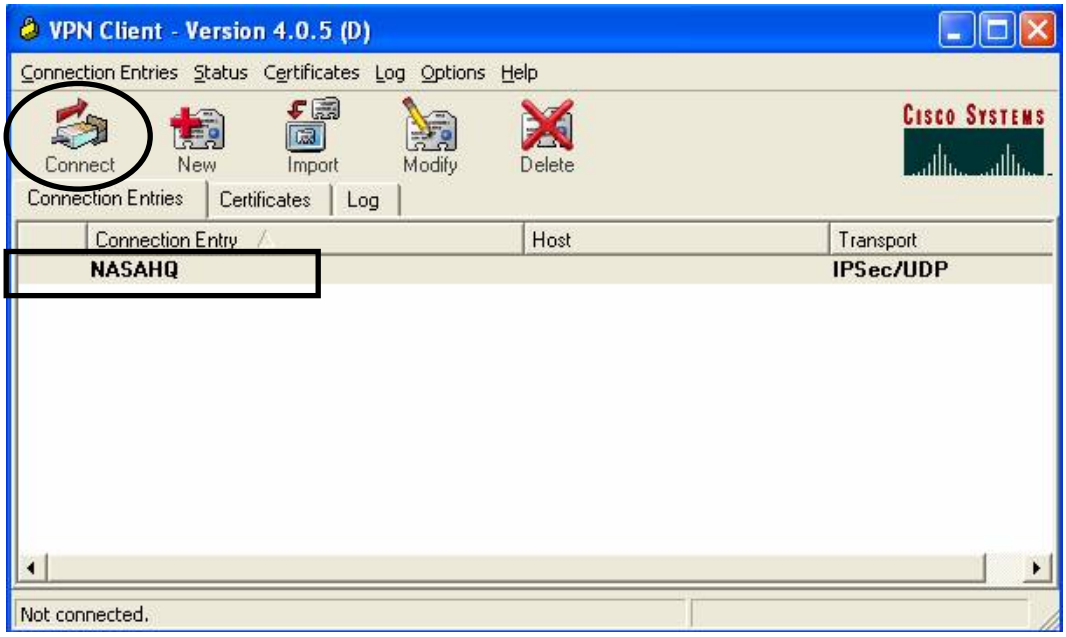
7.4 Virtual Private Network (VPN)

Connecting to the NASA HQ "**Virtual Private Network (VPN**)" requires a NASA-issued laptop. It can not be used from a personal or public-access computer. VPN gives users access to private network resources, such as file servers and internal Web sites. It is not necessary to use VPN to connect to NASA HQ publicly available services. **Note**: Access to the public Internet is required to access NASA HQ VPN.

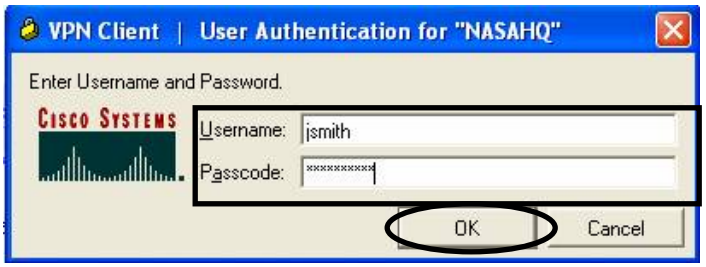
7.5 Using the Cisco VPN Client for Windows

1. Select "**VPN Client"** from start>Programs>Cisco Systems VPN Client.

2. The **"VPN Client"** window will open; select the desired connection from the **"Connection Entry"** field.
3. Click **"Connect"**.



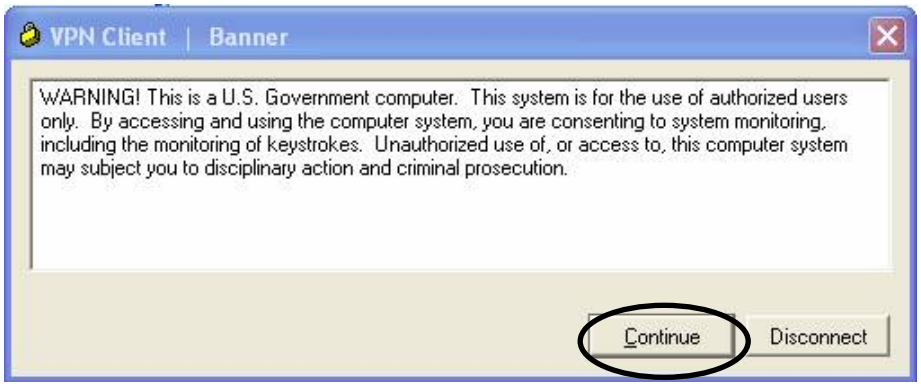
4. The **"VPN Client | User Authentication for "NASAHQ"** window will display.
5. Enter your HQ username in the "**Username:"** field.



6. In the "**Passcode:"** field, enter the **SecurID PIN+the 6-digit number on the token**.
7. Click **"OK"**.

Note: A **"VPN Client"** error message will display if a user exceeds the one minute time limit to enter the "**Username"** and "**Passcode"**.

8. Once connected, a **"VPN Client | Banner"** will display; click **"Continue"**.



9. If the **"VPN Client Authentication"** window did not display automatically, click the VPN padlock icon in the taskbar.
10. Select **"VPN Client**" from the pop-up menu.

11. Click "**Connect"** in the "**VPN Client"** window.

7.5.1 When I'm Connected, What Access Do I Have?

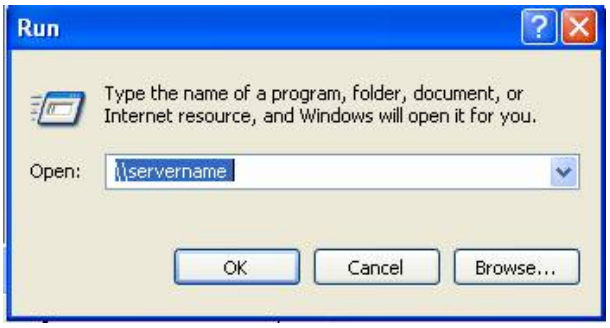
You will have access to the HQ private network and the Internet using TCP/IP. You can access internal Web sites such as NASA search pages, employee directories, and applications that are available through Internet Explorer.

7.5.2 How Do I Access My Network Files?

If using a NASA HQ laptop, the U:, X:, and other share drives will be available.

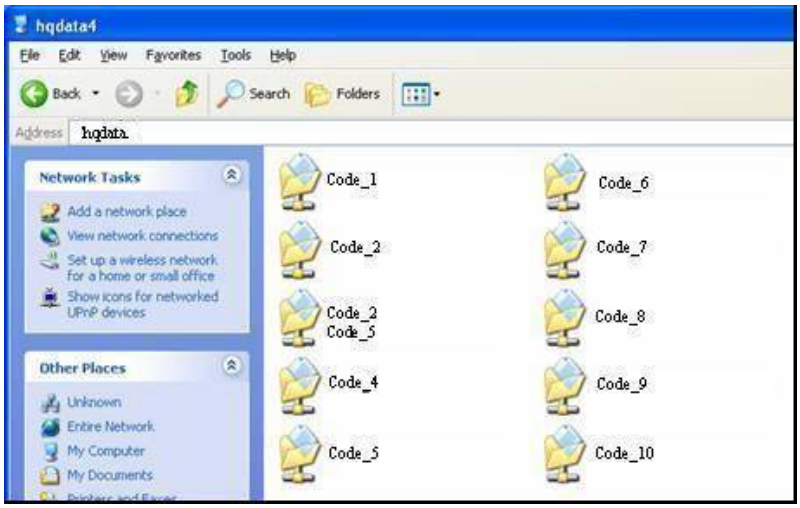
1. Select **"My Computer"** from the **"start"** menu or a desktop icon.

2. If unable to locate the U: drive, etc. in **"My Computer",** browse for the file server. Type the address, such as \\servername in the **"Address"** field of the "**My Computer"** window. Or select **"Run…"** from the start menu, and type in the **"Open:"** field.



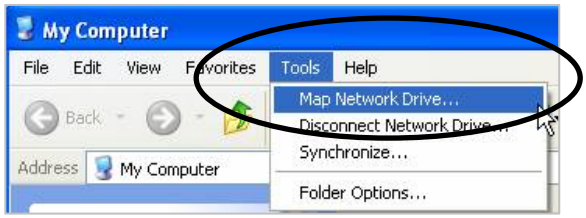
3. If prompted to connect, log on with your Windows (NT server) password **"(HQ\user ID)"**.
4. Click **"OK"**.

5. You should get a list of server shares; these contain your files. You can right-click on an individual share to create shortcuts or map server shares to drive letters.

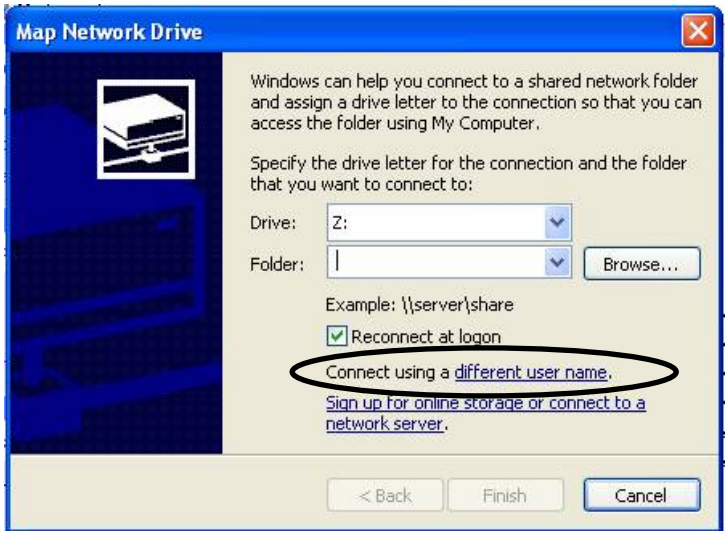


Note: If the above steps do not work, restart the computer, reconnect to VPN, and try the following:

6. Open **"My Computer"**.
7. Select: Tools >Map Network Drive…



8. From the **"Map Network Drive"** window, click **"Connect using a <u>different user name</u>"**.

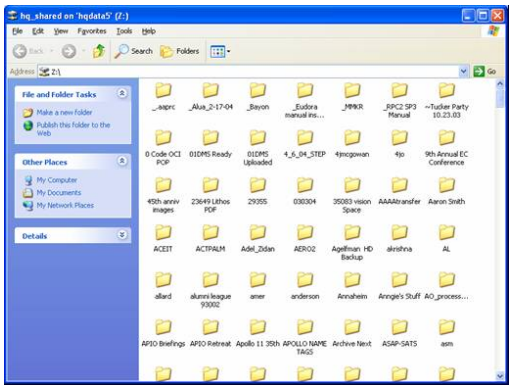


9. Log on with your **HQ\User Name** (as used in e-mail) with your Windows (NT server) password.
10. Click "**OK**".

11. From the **"Map Network Drive"** window, type the path to the file server share in the "**Folder:**" field in the format "<u>\\hqserver\share_name.</u>" If the path is unknown, it can be located under "**My Computer**" on your HQ PC at work, or call 1 (866) 4NASAHQ (TTY: 1 (866) 250-7680) or <u>service@hq.nasa.gov</u> to find out the path to use.

12. Mapping should take less than a minute to complete. If it fails, try again with attention to **username** and **password**.

13. The drive is mapped and ready to use.



Note: The VPN Client will disconnect after 4 hours, or when you log off or shut down your PC. Make sure to **save your work within 4 hours of connecting**, or more frequently if the VPN connection is left open.

14. To disconnect, quit all open applications and select "**Disconnect"** from the VPN Client menu or application window.

15. Disconnecting the VPN should restore your previous public Internet connection. If not, **restart** your computer.

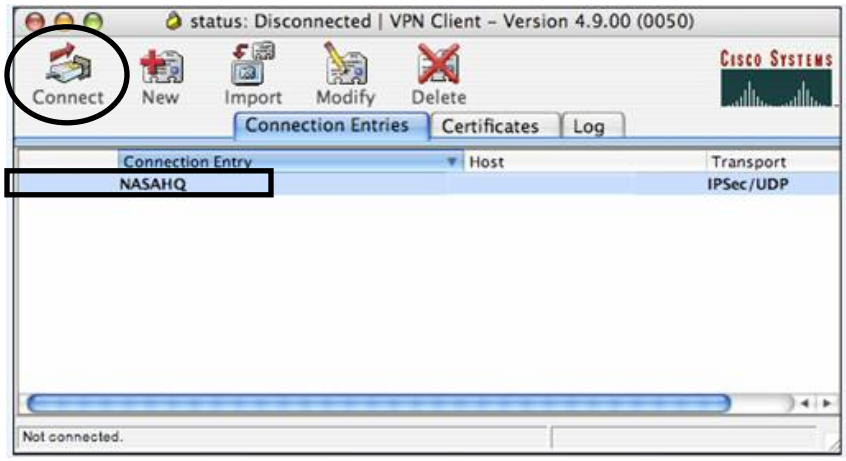
7.6 Using Cisco VPN for Mac OS X

You can connect to the NASA HQ "**Virtual Private Network (VPN)"** using Mac OS X. The VPN gives you access to private network resources, such as file servers and internal Web sites. You don't need the VPN to use NASA HQ publicly available services. **Note**: Access to the public Internet is required to access NASA HQ VPN.

1. Launch the "**VPN Client"** by clicking the **"VPN"** icon in the Dock.

2. If the "**VPN Client"** icon does not appear in the Dock, launch it from the "**Applications"** folder.

3. Ctrl-click the **"VPN"** icon in the Dock, and select **"Keep in Dock"** so the application can be launched from there.
4. The **"VPN Client"** window will open; select the desired connection from the **"Connection Entry"** field.
5. Click **"Connect"**.

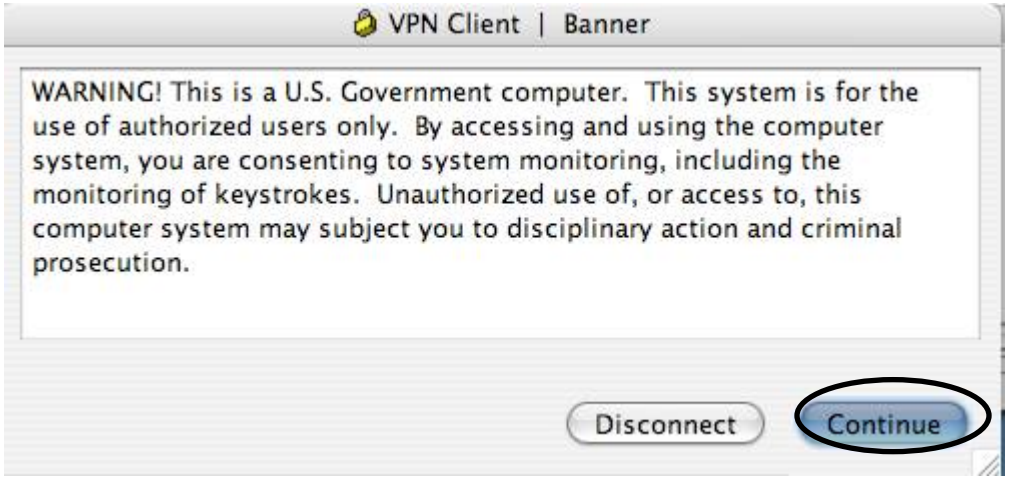


6. The **"VPN Client | User Authentication for "NASAHQ"** will display.

7. Enter "**Username**".
8. In the "**Passcode:**" field, enter the **SecurID PIN+the 6-digit number on the token**.
9. Click **"OK"**.

Note: A **"VPN Client"** error message will display if a user exceeds the one minute time limit to enter the "**Username**" and "**Passcode**".

10. If successful, the **"VPN Client | Banner"** will display; click "**Continue**".

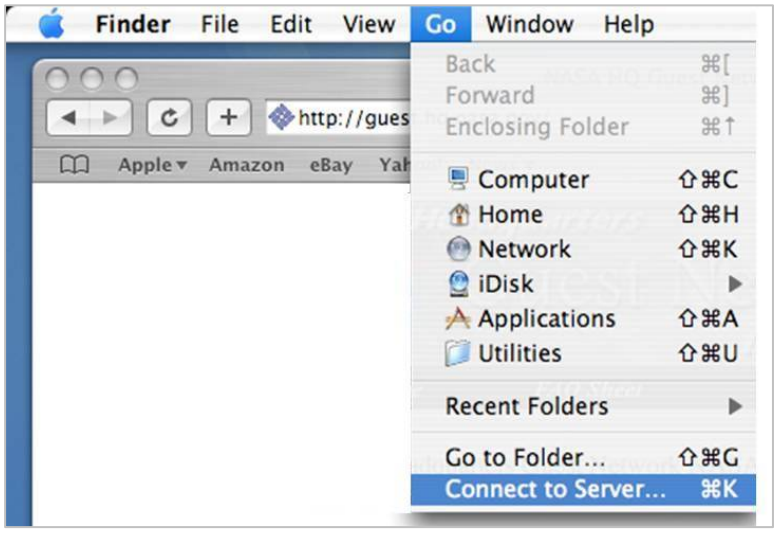


7.6.1 When I'm Connected, What Access Do I Have?

You will have access to the HQ private network and the Internet using TCP/IP. **Note:** AppleTalk is not supported on VPN; network servers and printers that use AppleTalk will be inaccessible. Refer to **"How Do I Access My Network Files?"** for instructions. You can immediately begin to use internal Web sites such as NASA search pages, employee directories, and other applications.

7.6.2 How Do I Access My Network Files?

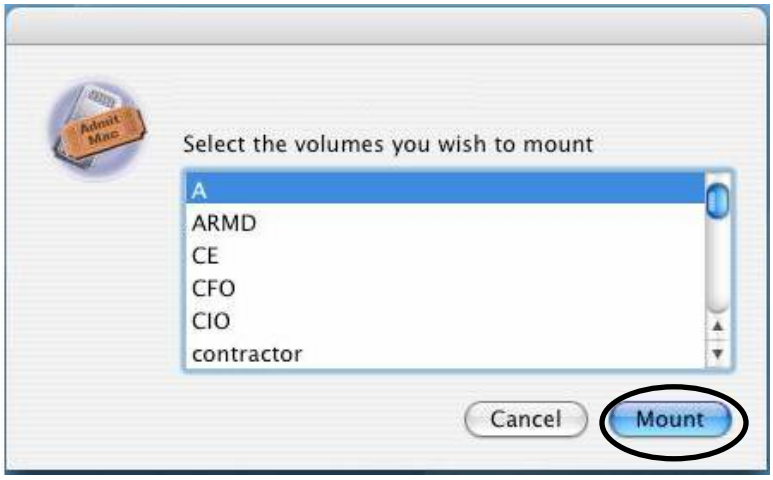
1. From the **"Go"** menu select **"Connect to Server"**. **Note:** To access network files requires knowing the name of the HQ server where they are stored.



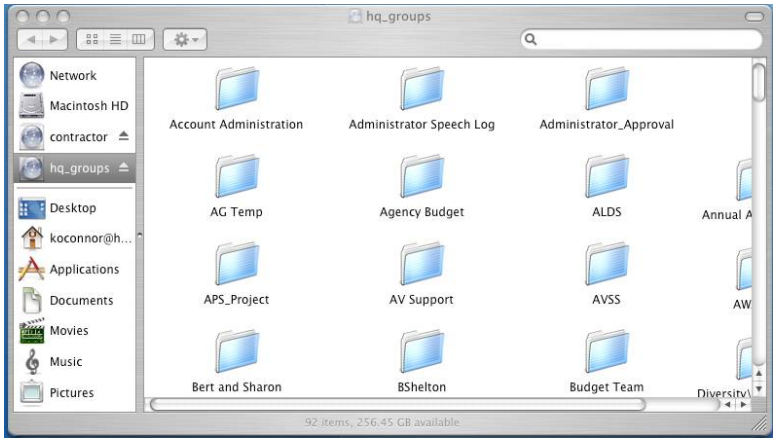
2. The **"Server Address"** window will display; enter the address to the server using this syntax: **smb://servername.hq.nasa.gov** (*servername* is the name of the server.).

3. Click **"Connect"**.

4. Select the share name to be mounted.
5. Click "**Mount**".



6. After selecting a share, an icon will appear on the desktop.
7. Double-click on an icon to access files and folders.

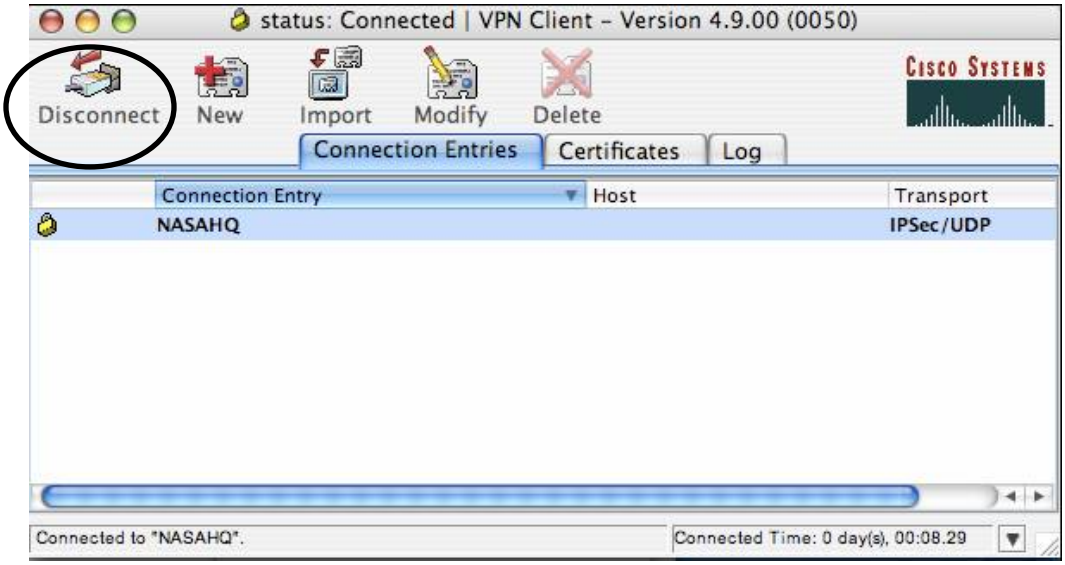


Note: If your Mac enters sleep mode, or is disconnected from the network, your VPN session will be terminated and an error message will display. Click **"Disconnect"**.

Note: To avoid being disconnected and losing unsaved work, eject the network shares before closing your screen, leaving your computer, or moving to a different location.

Quit all applications and click the "**Eject"** button in a Finder window.
If you attempt to shut down or log off your Mac, a **"VPN Client"** message will display.
If the network shares have been ejected, it is safe to select "**Disconnect and exit"**.

8. To disconnect manually, click the "**VPN"** icon in the Dock.
9. Click "**Disconnect"** after ejecting network shares, as described above.



10. The previous connection to the public Internet should be restored. If not restart the computer.

7.7 Known Issues with the VPN Method of Accessing HQ

Note: These comments apply to either Windows or Mac OS computers. Users connecting their NASA-issued laptop to DSL modems may encounter problems obtaining any high-speed Internet connection, and will be unable to use OWA, SNA, or VPN.

NASA's VPN service requires Dynamic Host Configuration Protocol (DHCP) to assign IP addresses or a known static IP address. Some modems that have been issued over the past few years have varied in type and quality, and a significant proportion of them are not DHCP enabled. While workarounds are often possible, each of the different types of modems requires a different solution. To obtain the correct instructions for your modem, work directly with your ISP.

If the modem is too difficult to work with, a user can invest in an "air card," available for purchase via PC Mall. Air cards are small devices that plug into a computer. They utilize cell phone technology rather than wireless access points and provide a fast, more reliable signal in most urban areas. An air card would make your laptop Internet-ready in any location where cell phones function.

7.8 Secure Nomadic Access (SNA)

Secure Nomadic Access (SNA) is a service that allows users to remotely access resources on the **"NASA HQ Network"** using a Web browser via a high-speed Internet connection.

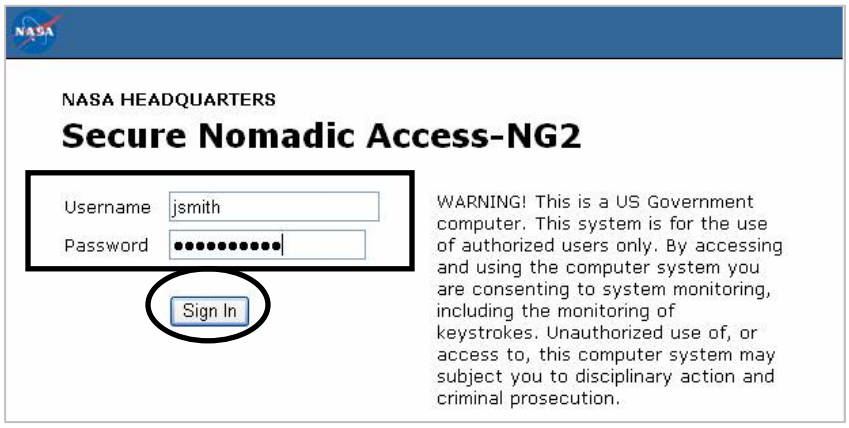
7.8.1 Logging On

The following are required to log in to SNA:

- A SecurID token and PIN
- JavaScript enabled in browser
- Cookies turned on in browser
- Access to the Internet
- HQ NT username and password for accessing network files

Follow these steps to log in to SNA:

1. Type the following address in your Web browser: https://sna.hq.nasa.gov .
2. Enter your NASA HQ **"Username**".
3. Enter the **SecurID PIN+the 6-digit number on the token** in the **"Password"** field, as shown in the next illustration.

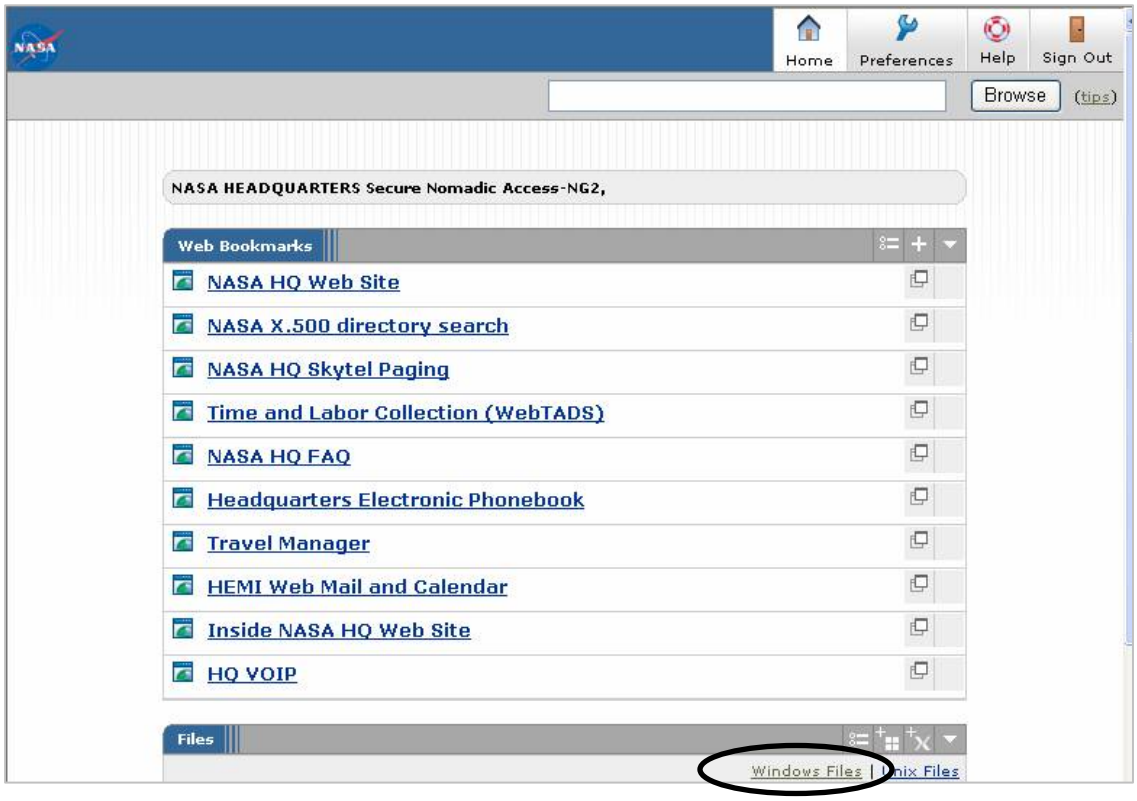


4. Click **"Sign In"**.

Note: If a blank Web page appears after entering the username and password, it may be because JavaScript is not enabled. JavaScript must be enabled for SNA to work.

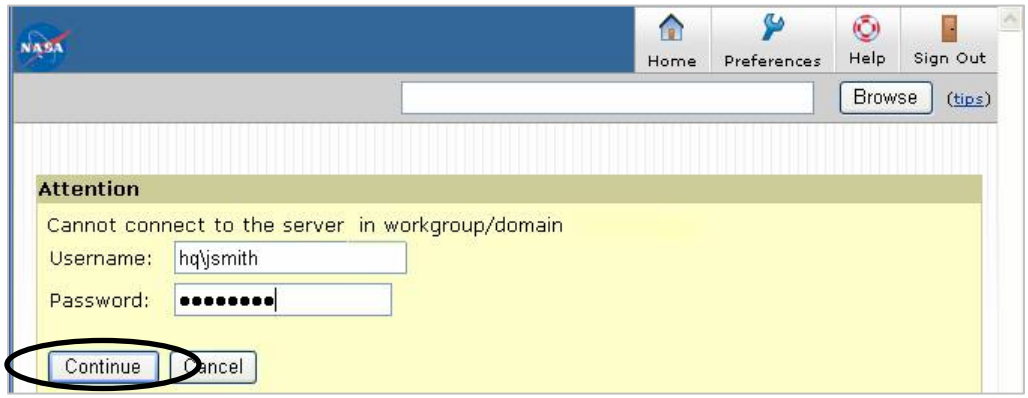
7.8.2 Accessing Windows Files (U, W, X Network Drives)

1. To access the U, W, or X drives, click the Bookmark for the drive; if none are bookmarked click **"Windows Files"** in the lower right corner.



Note: The following must be provided when prompted:

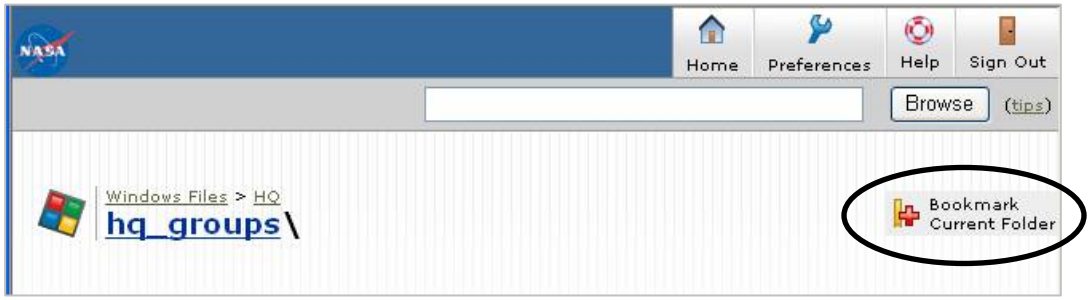
2. Type HQ\ then your HQ username in the **"Username:"** field (example: hq\jdoe).
3. Enter your HQ network password in the **"Password:"** field.
4. Click **"Continue"**.



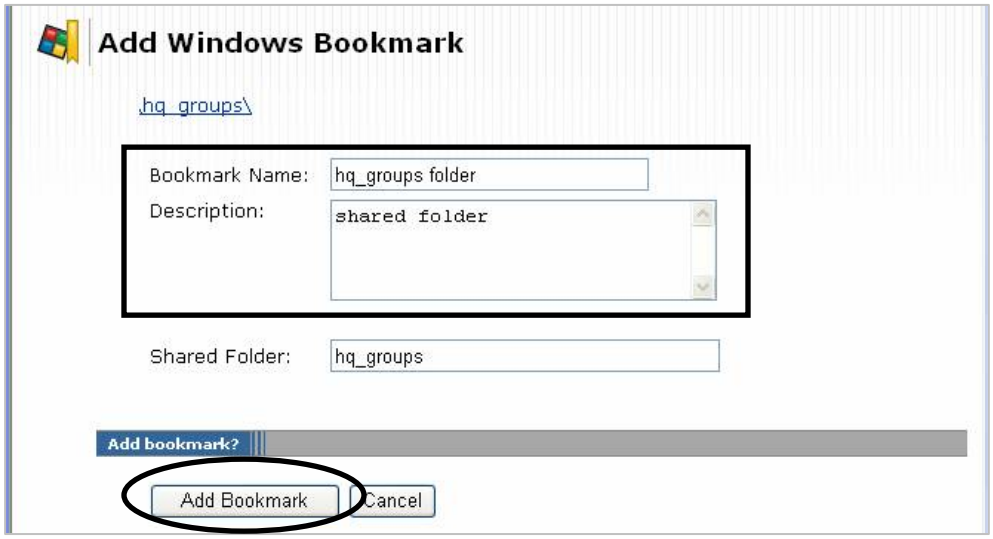
7.8.3 Creating Folder Bookmarks

To create bookmarks for frequently used folders:

1. Click **"Bookmark Current Folder"**.



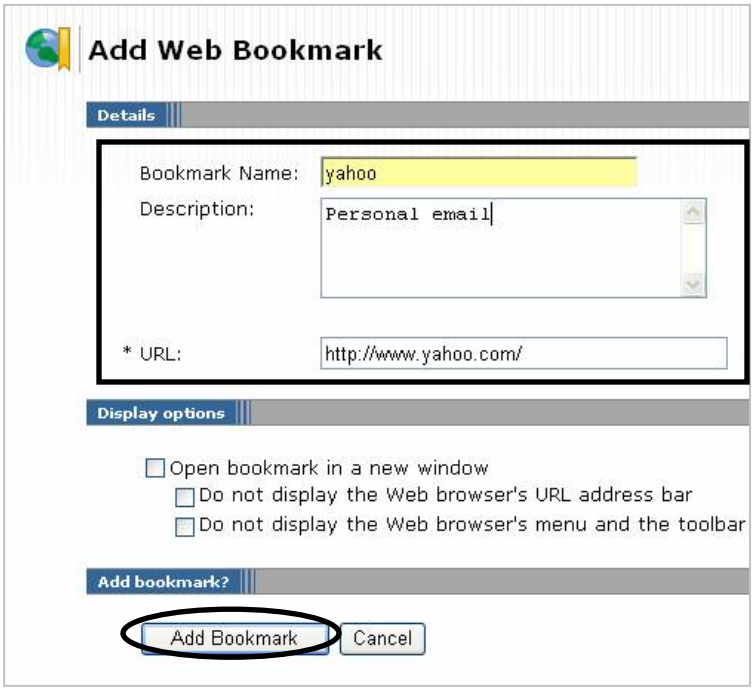
2. Enter a name for the bookmark in the **"Bookmark Name:"** field.
3. Enter a description for the bookmark in the **"Description:"** field.
4. Click **"Add Bookmark"**.



7.8.4 Add Personal Bookmarks

1. Click the plus sign in the **"Web Bookmarks"** toolbar.

2. Enter a name for the bookmark in the **"Bookmark Name:"** field.
3. Enter a description of the bookmark in the **"Description:"** field.
4. Enter the URL in the **"URL"** field. **Note:** Use the following format: http://www.hq.nasa.gov/office/codec/ .

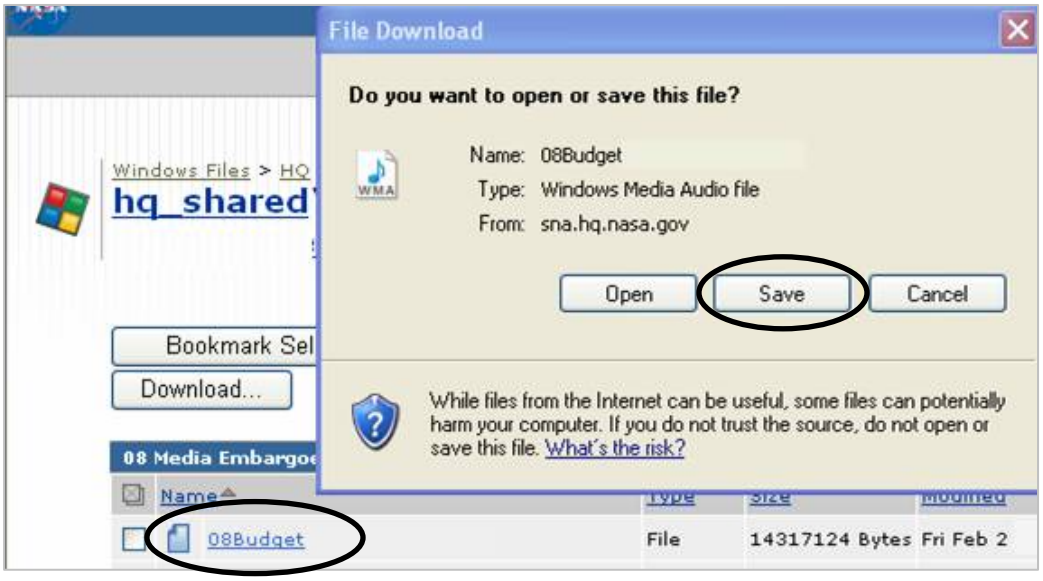


5. Display options can be selected in the **"Display options"** field.
6. Click **"Add Bookmark"**.
7. To delete a bookmark, click the trash can symbol located on the right of the toolbar.

7.8.5 Opening Files

1. Click the link of the file to be opened.
2. Click **"Save"**.

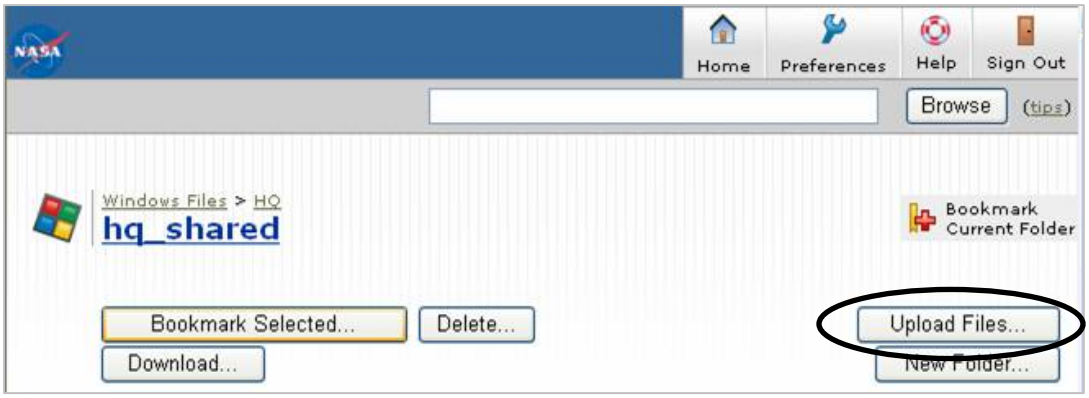
Note: The browser will either open the file with an application or prompt you to save it. If prompted to save the file, it is recommended that you save it to the desktop of your computer.



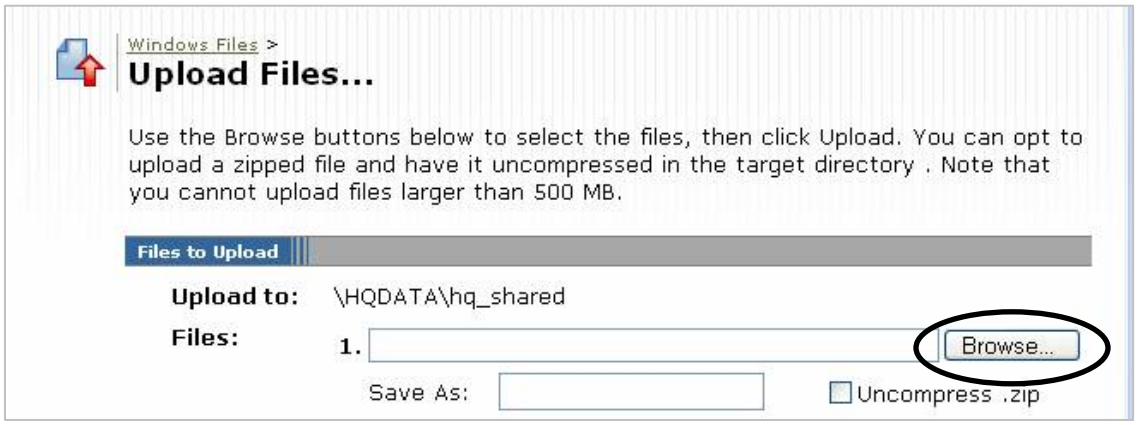
7.8.6 Uploading Files

To bring files into SNA from a local machine:

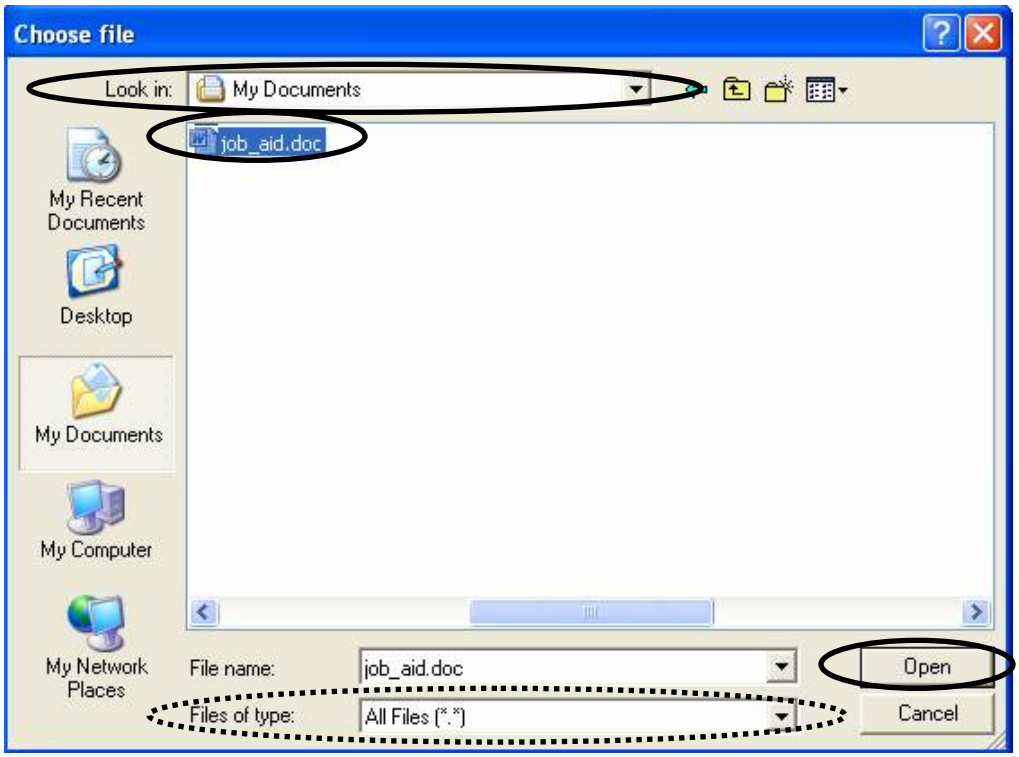
1. Click **"Upload Files…"**.



2. Click "**Browse…**".

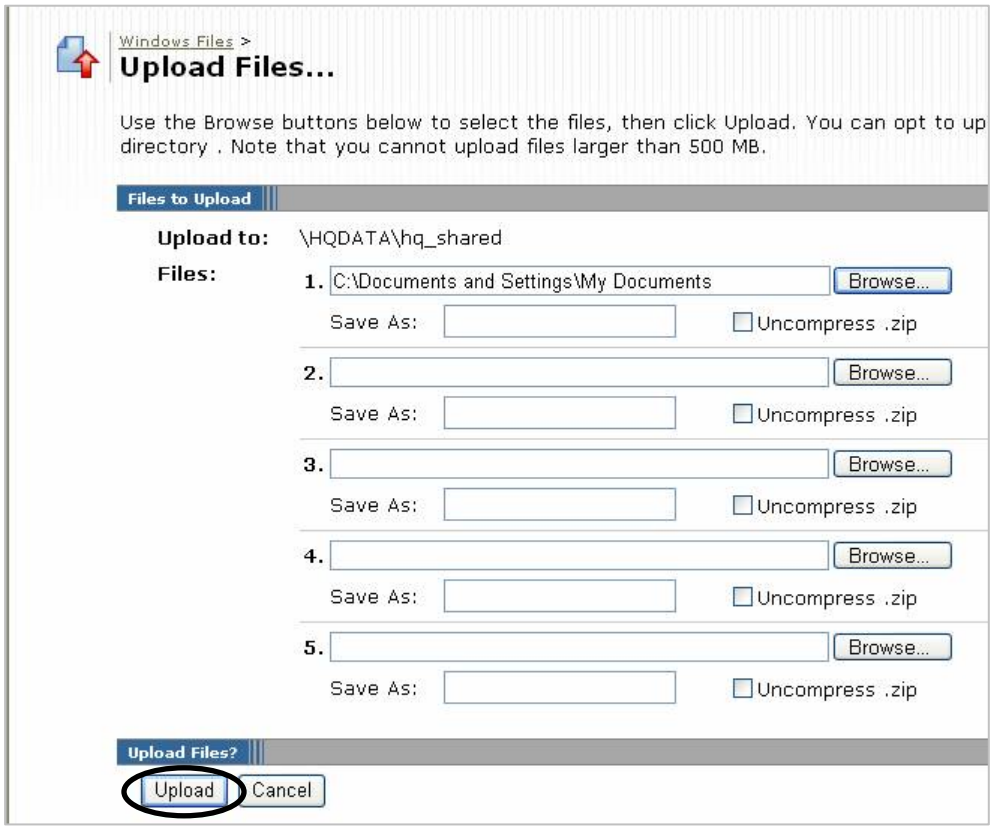


3. The **"Choose file"** dialog box will open; select the folder and file to be uploaded.
Note: The "**Files of type:"** selection may have to be changed.

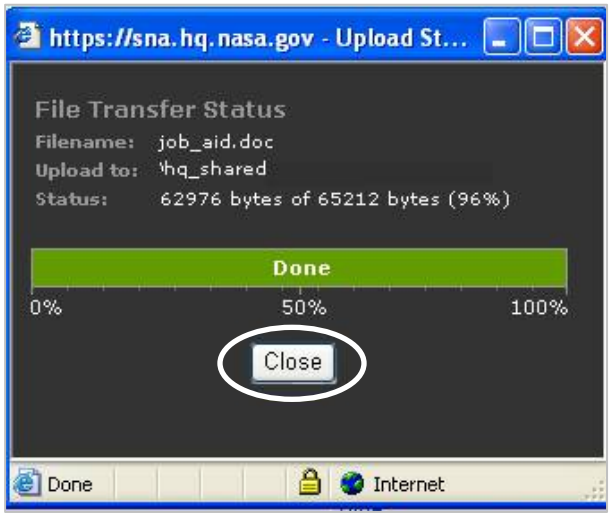


4. Click "**Open**".

5. Click "**Upload**".



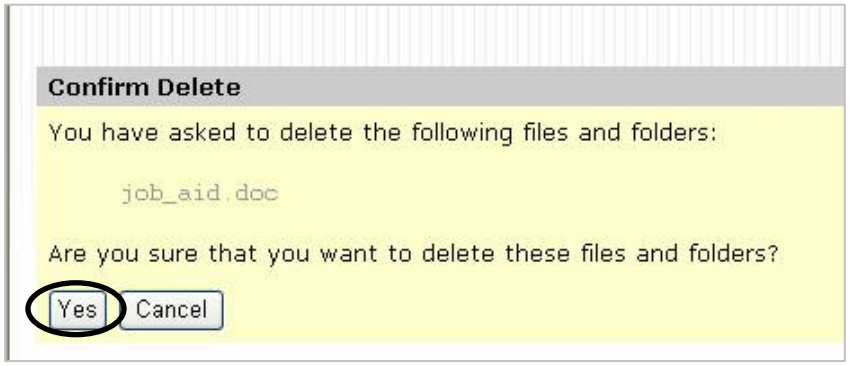
6. A **"File Transfer Status"** window will open showing the file has been uploaded.
7. Click **"Close"** to exit.



7.8.7 Deleting Files

1. Click the checkbox next to the name of the file(s) to be deleted.

2. Click **"Delete…"**.
3. A **"Confirm Delete"** message will display; click **"Yes"** to delete.



7.9 SNA Frequently Asked Questions

What happens after I log in?

SNA will open to a main page where all services provided by SNA can be accessed. Each Organization at NASA HQ has its own File Bookmarks; each user with an SNA account will be placed in the appropriate Organization group.

My SNA connection was broken but I didn't log out. What happened?

There is a 4 hour time limit for SNA sessions at which point you will be automatically disconnected. **Note:** A warning message will display before disconnection.

Can I log in to SNA more than once?

You can not log in to SNA from multiple computers at the same time. You can open multiple browser windows and have them open to SNA at the same time once you have logged in. This allows you to access multiple internal HQ resources at one time.

How do I report applications that work (or don't)?

Send an e-mail to sna-comments@hq.nasa.gov to provide feedback on Internal HQ applications that you use but are not listed above. Please provide the following information:

- Operating System
- Web browser and version
- URL used to access the application
- Screenshots of any error messages encountered
- Date and time testing occurred

Can I get training?

For general training, call the Computer Training Center (CTC) at (202) 358-1111. The CTC performs group and 1-on-1 desk-side support.

Can I access my C: drive with SNA?

No, it is not possible. Any documents to be accessed through SNA must be saved on a shared drive, and then it can be accessed from SNA.

How do I log out of SNA?

Log out or quit any Web applications that are running through SNA. Click the **"Sign Out**" button in the upper right corner of the SNA page or any page. **Note:** The same **"Door"** icon will appear in the right corner of any page that is opened through SNA.

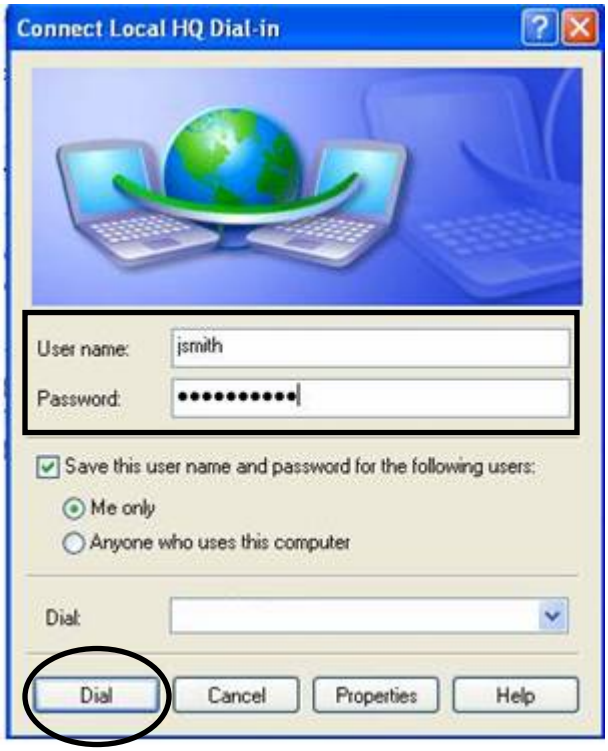
7.10 Dial-Up

This provides instruction for **"Dial-Up"** Internet connection. To obtain the phone numbers for dialing in to NASA HQ IT Resources, please call the Help Desk.

7.10.1 Windows XP Remote Access

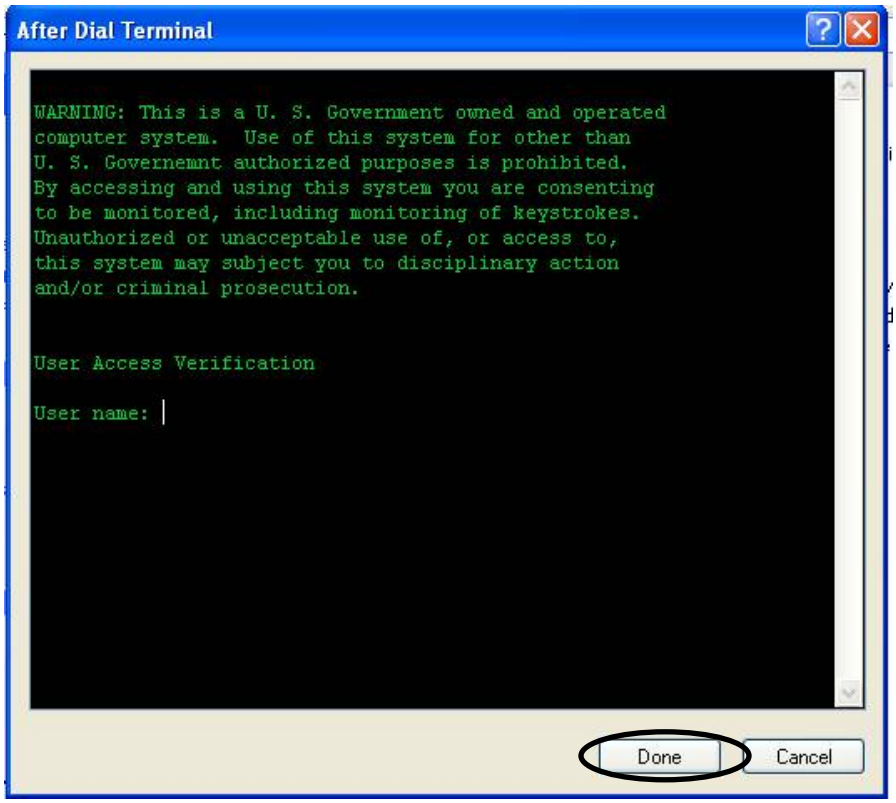
Users who use dial-up to connect to an Internet Service Provider (ISP) are unable to access the NASA servers because the NASA HQ Domain Name Servers (DNS) are behind the NASA HQ firewall. If an analog phone line will be used to connect, use the following instructions:

1. In the **"Dial:"** field, enter the number that has been provided.
2. If using an ISDN line, enter the NASA HQ user ID in the **"User name**" field.
3. Enter SecurID PIN+the 6-digit number on the token in the **"Password"** field.
4. Click **"Dial"**.



5. The computer begins the connection process.

6. After a connection has been established, a terminal window will display; enter your NASA HQ user ID after the **"User name:"** prompt.



7. Click **"Done".**
8. The **"Connecting Local HQ Dial-in…"** window will display; once the username and password are verified, you will be connected to NASA HQ.

7.10.2 Known Issues with Dial-In Method of Accessing HQ

Your computer name must be registered with the NASA HQ domain server in order to gain full functionality from dial-in. If your computer name is not registered with the HQ domain server, you will only be able to access e-mail and Internet services—not the network file shares.

7.10.3 Disconnecting from the NASA HQ Dial-Up Network

1. Locate the **Windows Tray** on your screen (usually in the bottom right corner of your task bar).

2. Right-click the **"Dial-Up Status Monitor"** icon (looks like two computers).
3. Select **"Disconnect"**.

7.11 Macintosh Remote Access (Dial-In)

Macintosh Dial-In instructions have not been approved. If you have any questions, contact the IT Help Desk at (202) 358-HELP (4357) or 1 (866) 462-7247.

7.12 Shared Drives

Network Structure		
Function	Macintosh Feature	PC Feature
Local hard drive	Macintosh HD	**C: Drive** Located inside *My Computer* icon, which is on the **Desktop**
Folder on the server where all users have full rights to read, copy, and delete files. Temporary 60-day storage.	hq_shared	**X: Drive** Located inside *My Computer* icon, which is on the **Desktop**
Folder on the server that contains all the workgroup folders. These folders are cross-organizational and users from different organizations may have permissions to access their contents.	hq_groups	**W: Drive** Located inside *My Computer* icon, which is on the **Desktop**
Your Organization's folder on the server. These folders have been renamed to reflect the transformed organization names (CFO)	CFO	**U: Drive** Located inside *My Computer* icon, which is on the **Desktop**
Alias to your private folder on the server.	Home folder Alias on the Desktop	**T: Drive** A shortcut on the **Desktop** identified with your user name

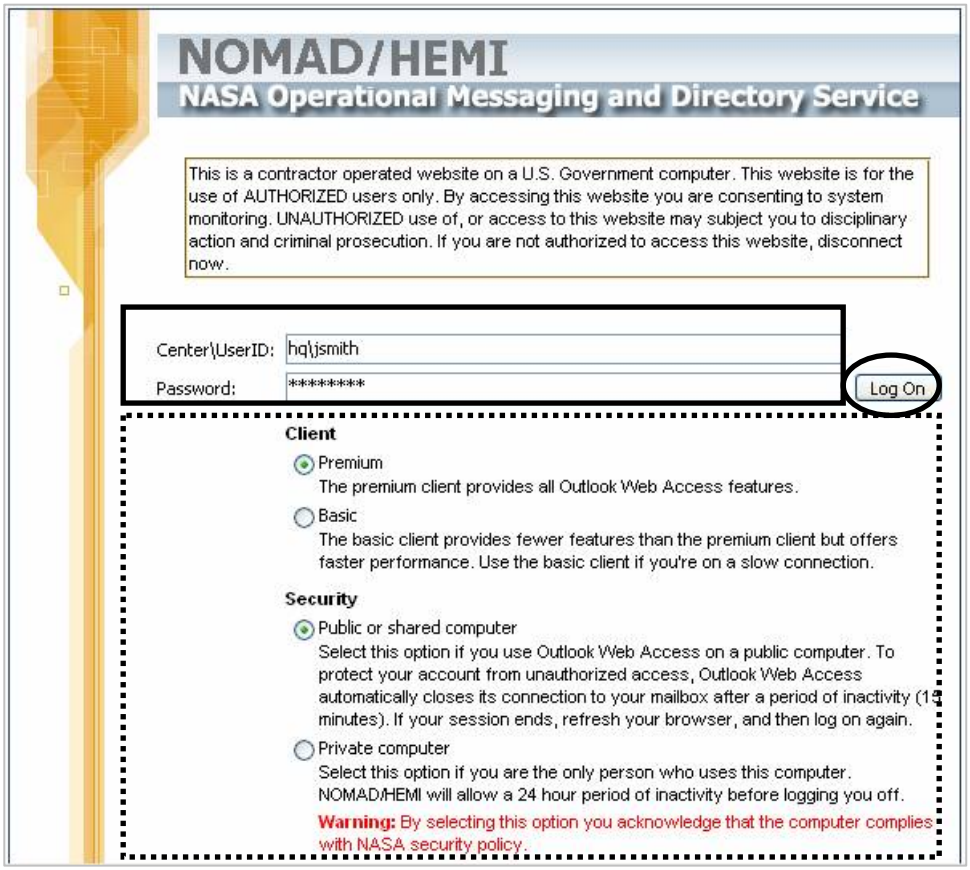
8 Outlook Web Access (OWA)

Outlook Web Access (OWA) allows users to access e-mail and calendar from a remote location using the Internet and a Web browser.

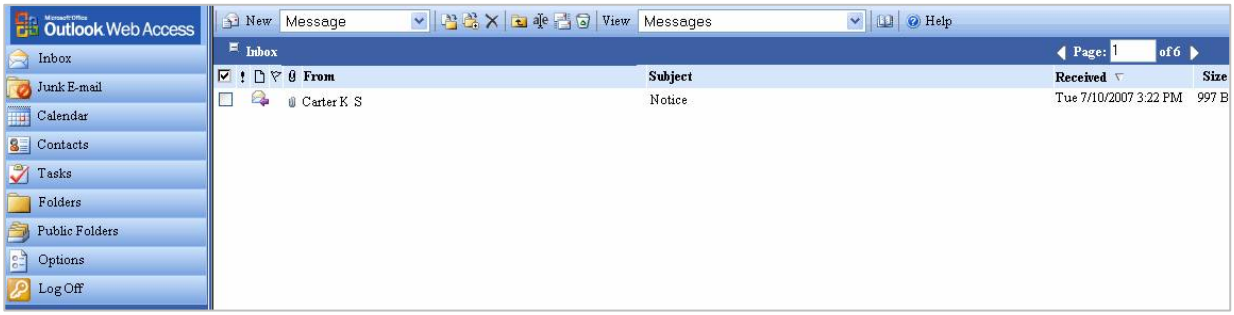
For PC users, Internet Explorer version 6.02 is the preferred browser and version for OWA due to software compatibility. **Note:** To check your IE version, from the Internet Explorer toolbar go to: Help>About Internet Explorer. A window will open displaying the version information.

For Mac users, Safari version 2.0.4 is the preferred browser and version for OWA due to software compatibility. **Note:** To check your Safari version, from the Safari toolbar go to: Safari>About Safari. A window will open displaying the version information.

1. Enter the following URL: https://webmail.nasa.gov in the address bar.
2. In the **"Center\UserID:"** and **"Password:"** fields, enter your HQ domain username and password, use the format hq\username.
3. Check the appropriate selection for **"Client"** and **"Security"** based on the computer being used. **Note:** Client selection is unnecessary for Mac users. Regardless of the selection, only the **"Basic"** client view will display.
4. Click **"Log On"**.



This is an example of the **"Basic"** Webmail client. **Note:** The basic client provides fewer features than the premium client, but offers faster performance. Use the **"Basic**" client if using a slow connection.



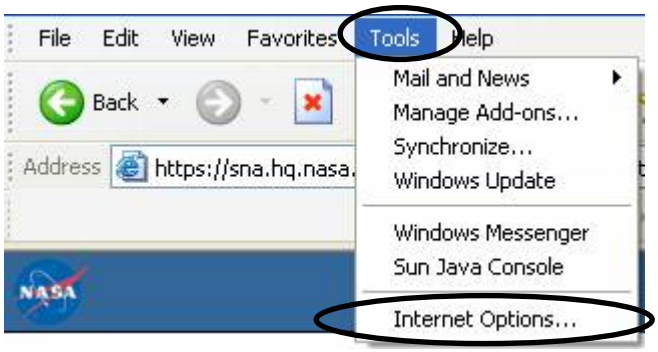
9 SharePoint

Microsoft SharePoint is a powerful, online tool for information sharing and document collaboration. SharePoint is easy to use, requires minimal training, and is available Agency wide. It uses a familiar browser interface and is tightly integrated with Outlook, Word, Excel, and other Microsoft Office products routinely used by employees.

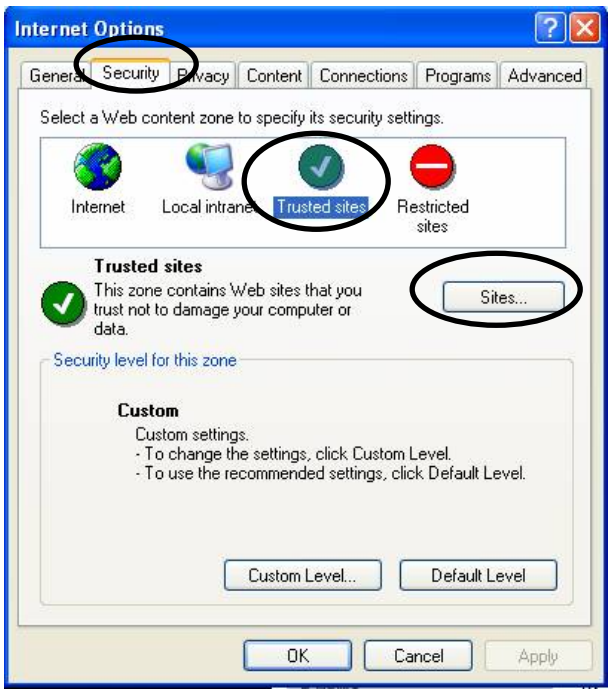
9.1 How to Add SharePoint to Trusted Sites in Internet Explorer

Adding SharePoint to your "trusted sites" allows your user ID and password to pass through to SharePoint when you log on to your computer, eliminating the need to log on again. It also allows SharePoint to interface with Microsoft Office at the most efficient level.

1. From the Internet Explorer toolbar, select: Tools>Internet Options…

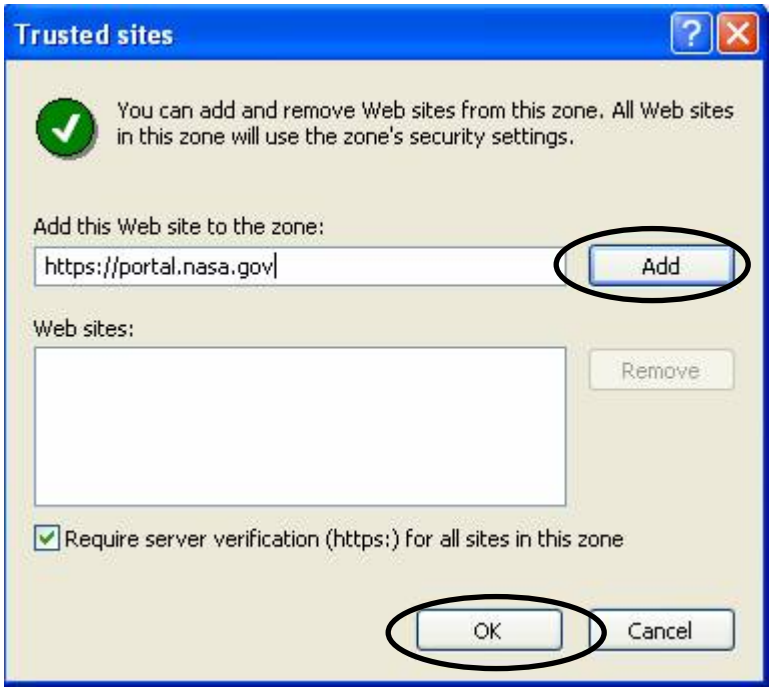


2. Select the **"Security"** tab.
3. Click **"Trusted sites"**.



4. Click **"Sites…"** and the **"Trusted sites"** window will open.

5. Enter https://portal.nasa.gov and click **"Add"**.



6. Click **"OK"** to exit and close.

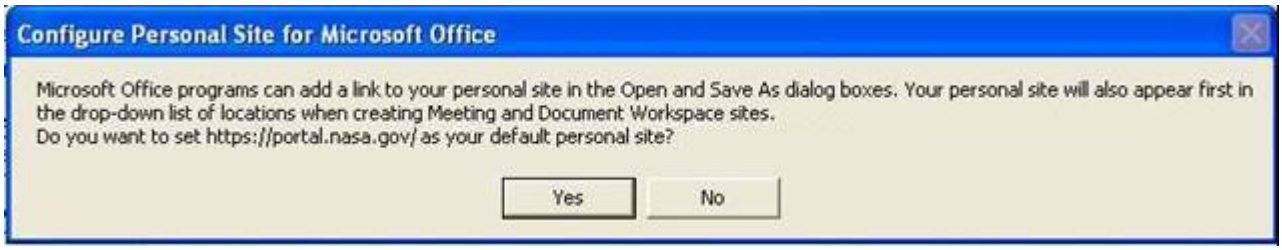
9.2 Using the SharePoint Document Library

1. To log on to NASA SharePoint Portal, go to https://portal.nasa.gov.

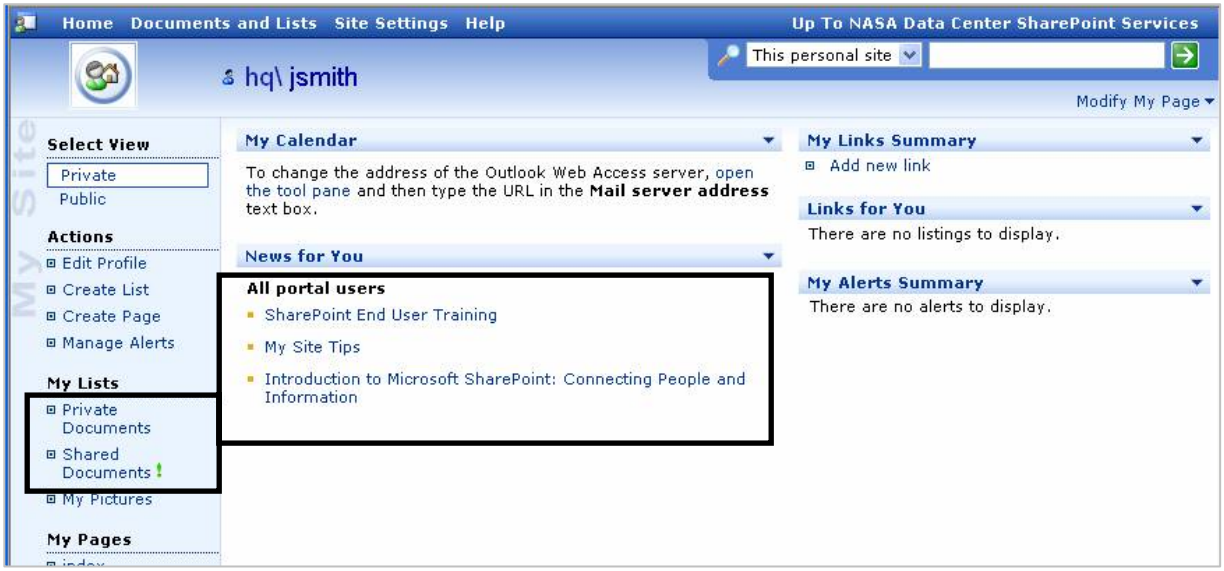
2. If you have logged in to SharePoint before, you may be automatically logged in. If not, enter your HQ username in the format hq\jdoe2 and your HQ password. Click **"OK"**.

3. Click on **"My Site"**.

Note: If you have not configured your personal site, a message will display asking if you want to add a link to your personal site. Select **"Yes"** or **"No"**. This makes adding documents created locally to your SharePoint document library more convenient, as you can do so from within applications such as Microsoft Word or Excel.

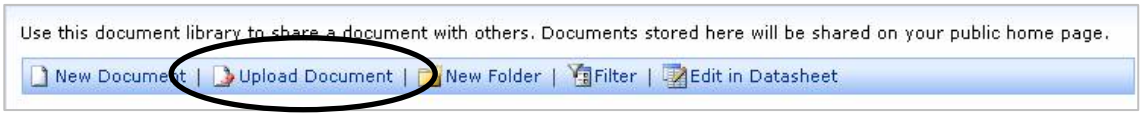


3. Important links for **"SharePoint End User Training"**, **"My Site Tips"**, and **"Introduction to Microsoft SharePoint: Connecting People and Information"** can be found under **"News for You"**.
4. In the left pane, there are links to upload **"Private Documents"** and **"Shared Documents"**.

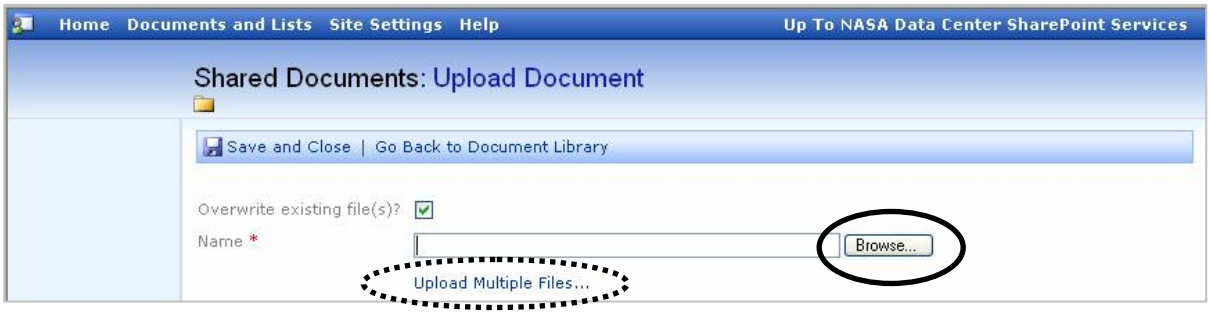


Note: To share documents with other NASA SharePoint users, they must be uploaded to the shared document workspace or to the **"Shared Documents"** within your Site. After uploading the document, access must be granted for others to view and/or edit the document.

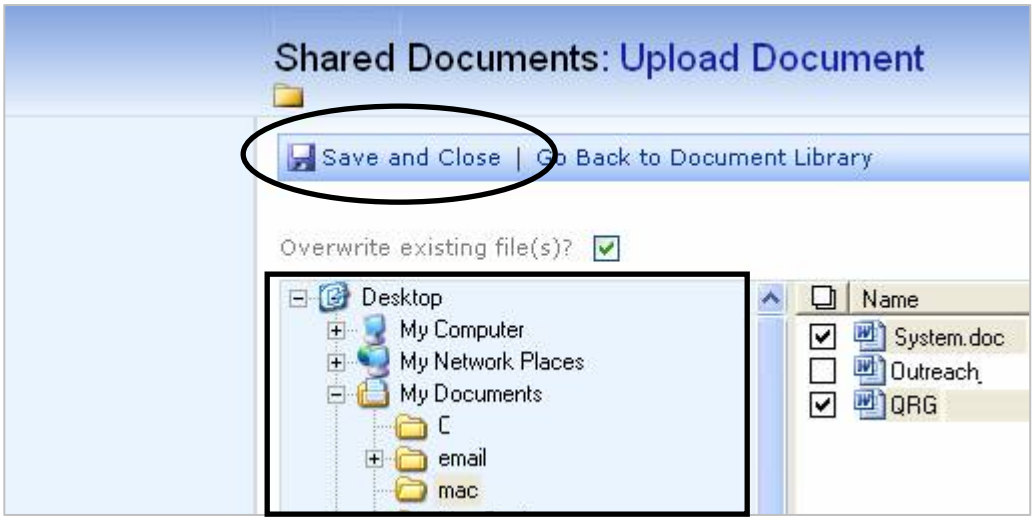
5. To upload a document, click on the **"Shared Documents"** link.
6. Click **"Upload Document"**.



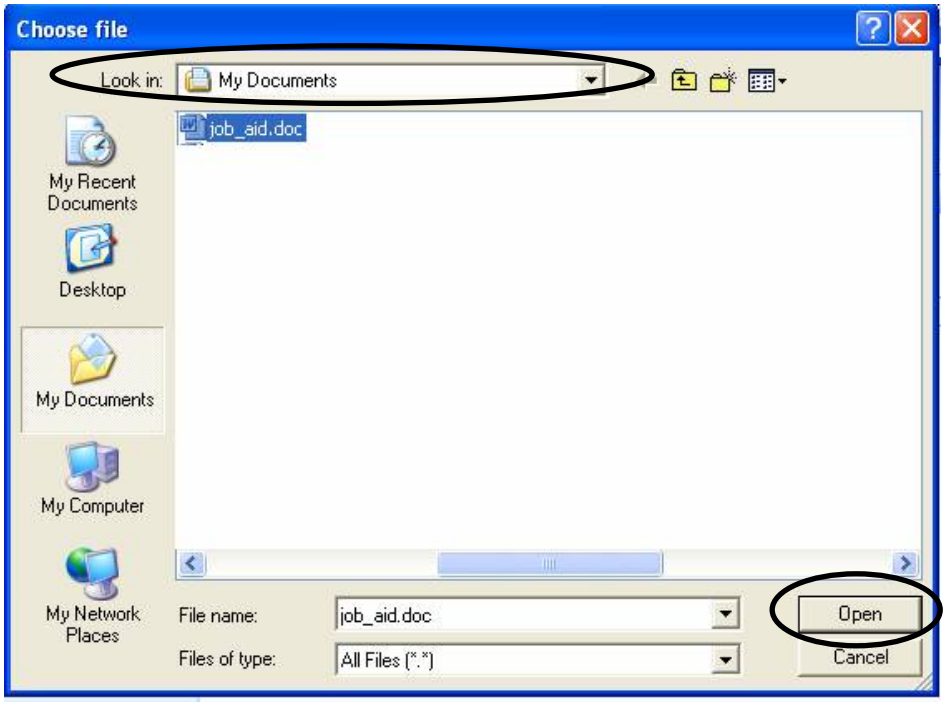
7. Click on the **"Browse…"** button to select the document to upload to SharePoint.



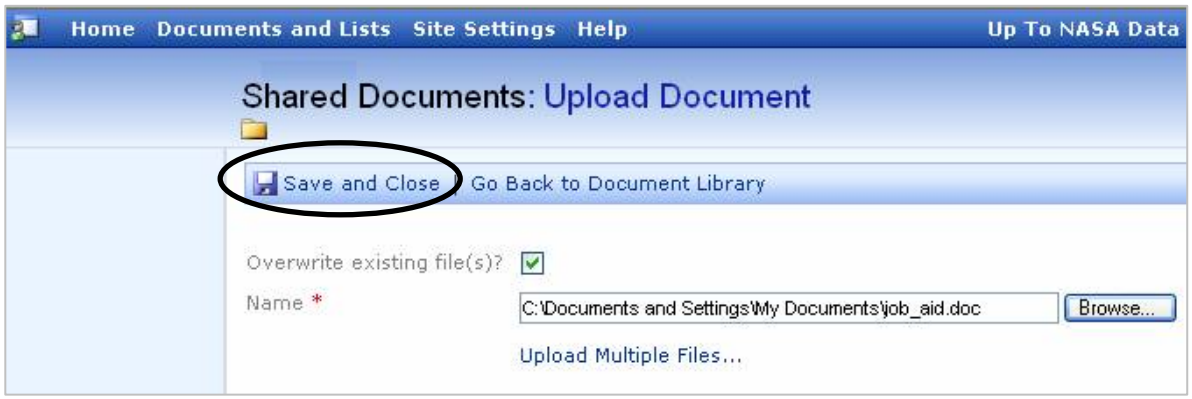
Note: To upload multiple documents, click on the **"Upload Multiple Files…"** link**.** Use the Explorer window to choose the folder and files to be uploaded. When done, click **"Save and Close"** as shown in the illustration below.



8. If you have selected to browse for a single file, the **"Choose file**" window will display; select where to browse for the file in the **"Look in:"** field.
9. Once located, select the file and click **"Open"**.



10. The path and filename of the document to be uploaded are now listed in the **"Name*"** field.
11. Click **"Save and Close"** to complete the upload process.



12. After uploading the document(s), access must be granted. To grant access to other SharePoint Portal users, select **"Site Settings"**.

13. Select **"Go to Site Administration"**.

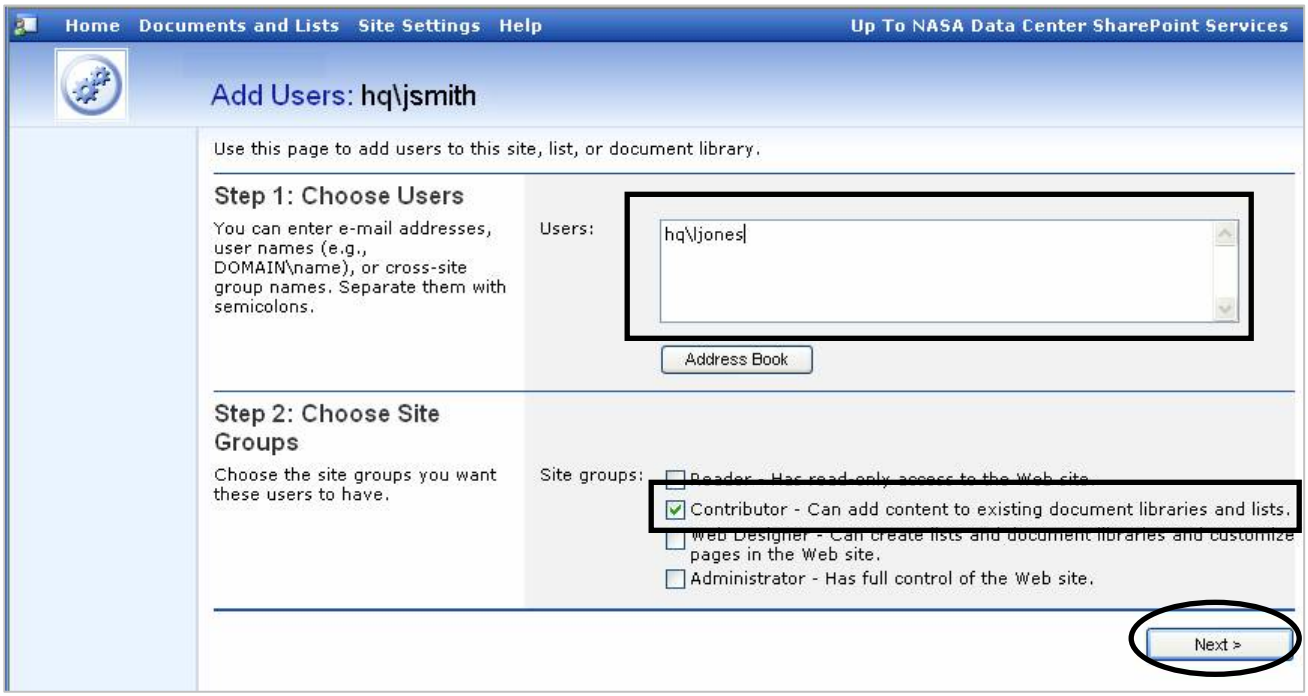
14. Click **"Manage site groups"**.

15. Click on the "**Contributor"** text link. **Note:** Do not click on the check box to the left of **Contributor**.

16. Click **"Add Members"**.

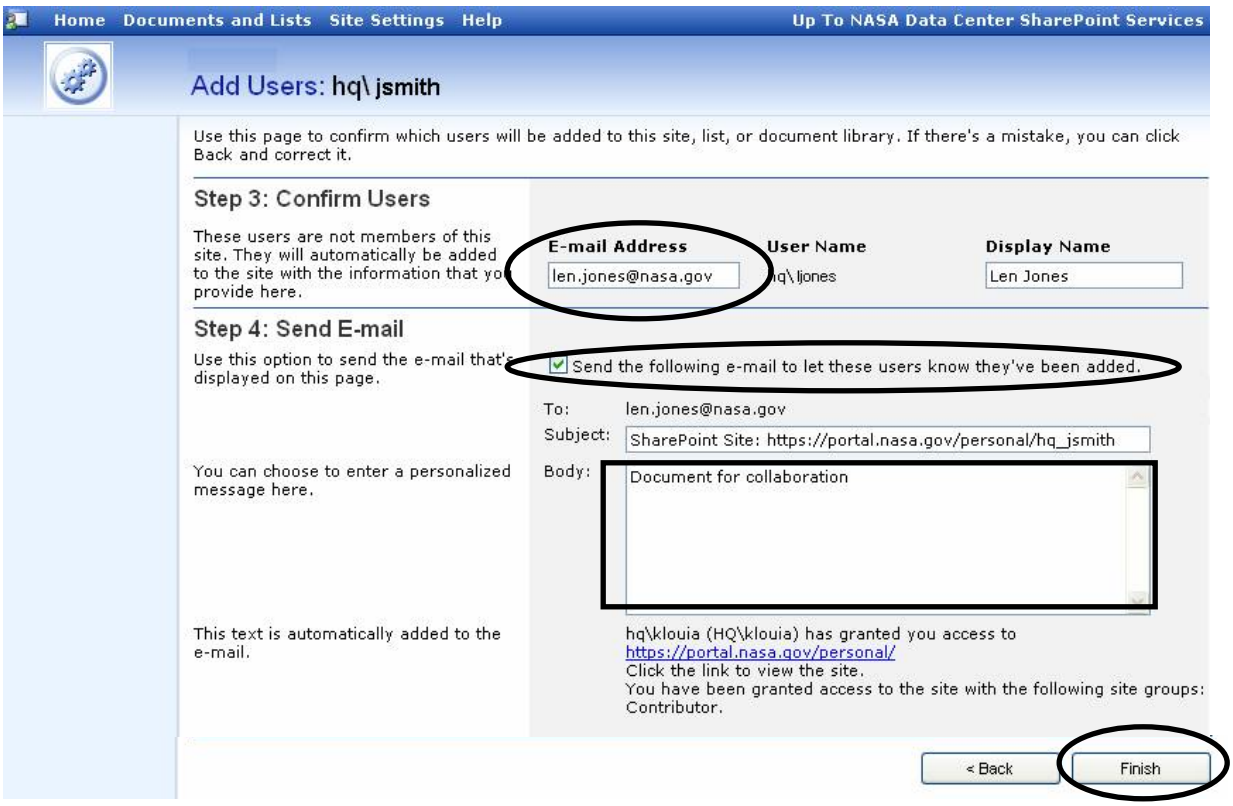
17. Add member(s) using the following format: HQ\user ID. **Note:** This format must be used or sharing will not work properly. If the user ID is unknown, locate the correct user ID from X.500.

18. Click **"Next"**.



19. Once added, make sure the **"Contributor"** role is checked.
20. Click **"Next"**.

IMPORTANT: DO NOT add users with e-mail addresses or the **"Address Book"** button. Users from NASA domains that have a trust with the NDC domain can be granted access to SharePoint using their local domain account. As of 11/06, those domains are: ARC, GSFC, GRC, LaRC, HQ, KSC, JSC, MSFC, SSC and WSTF. For the latest list of trusted domains, contact Nancy Kabakjian at (256) 544-2720. Users from other NASA domains must apply for an NDC domain account.



21. Enter the OneNASA e-mail address in the **"E-mail Address"** field.
22. Check **"Send the following e-mail to let these users know they've been added"**.
23. Compose the message in the **"Body:"** field.
24. Click **"Finish"** to add the user and send the e-mail.

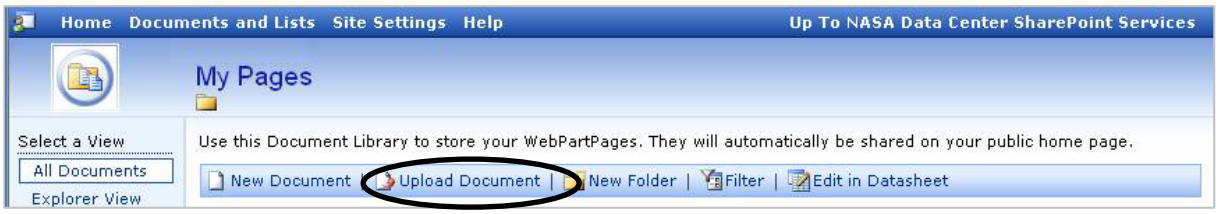
25. The added user now appears under the **"Users"** list.

9.2.1 Working with Document Libraries in SharePoint

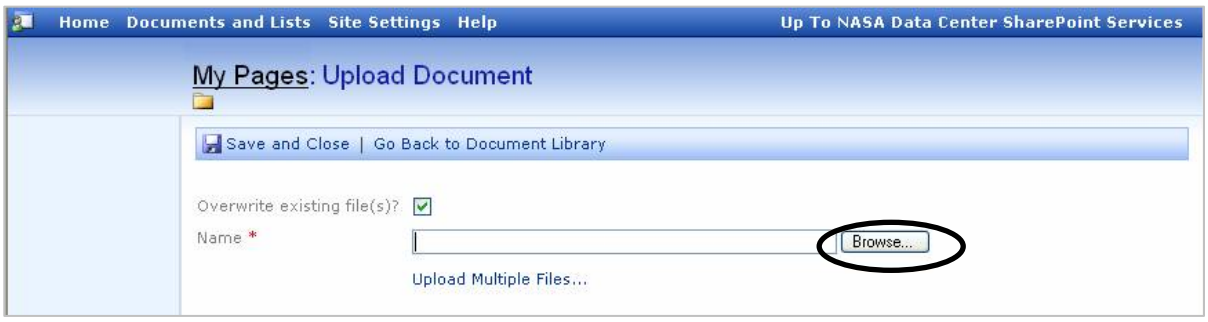
1. From the SharePoint home page, select **"Documents and Lists"**.

2. Select the folder where the document should appear.

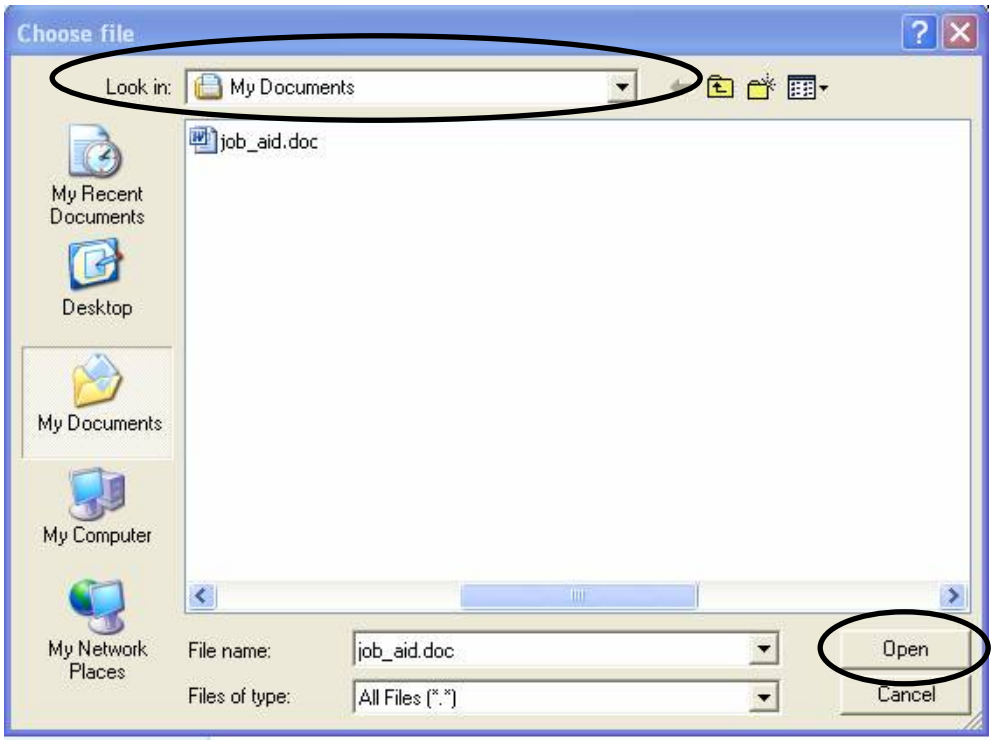
3. Click **"Upload Document"**.



4. Click **"Browse…"** to navigate to the file.

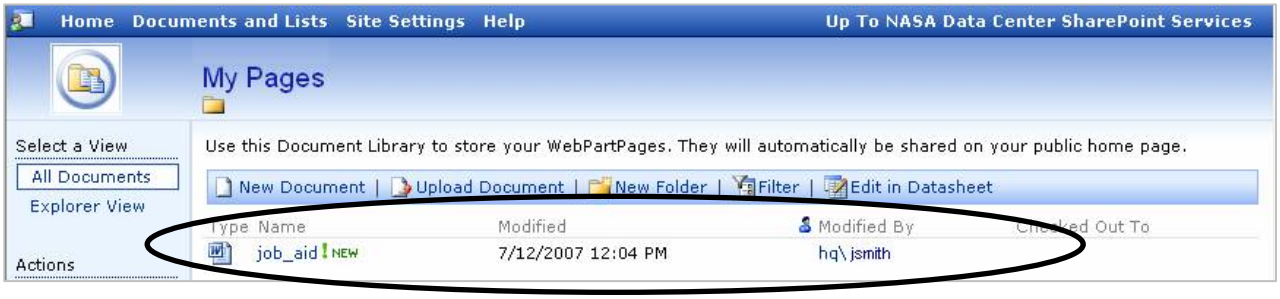


5. The **"Choose file"** window will display. Select where to browse for the file in the **"Look in:"** field and click **"Open"**.



6. Click **"Save and Close"**.

7. The document now appears in your library.



9.2.2 About SharePoint Document Check Out and Check In

A SharePoint document library requires files to be checked out for editing and then checked back in when the edits are complete. This enables the document owner to track changes that have been made to the document and by whom.

Document Check Out
When a document is checked out, it can not be edited by other users; also, they will not be able to see the changes until the file is checked in and it is approved by the site administrator. If you decide to check in the document without saving the changes, you can use the **"Discard changes and undo check out"** option on the Check In page. The document reverts to the last checked-in version, and no version history is kept for the unsaved changes.

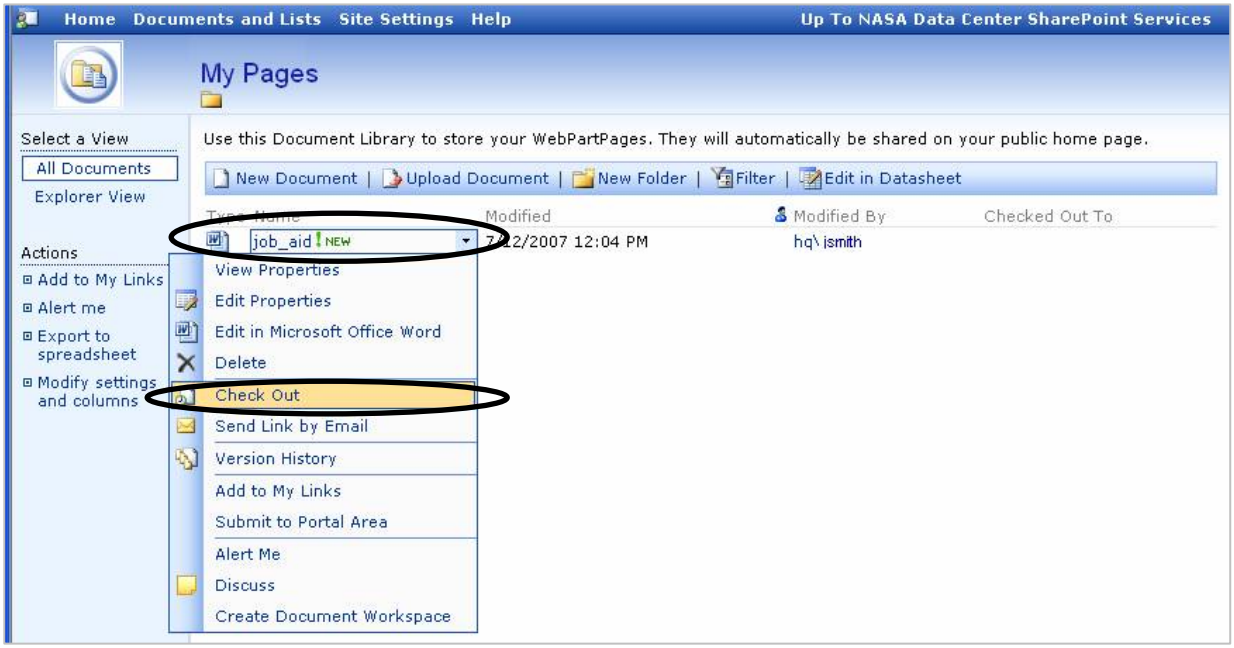
Note: Once a document is checked out, it must be opened in the appropriate application (Word, Excel, etc.) from the same menu as the Check Out command.

Document Check In
Once the changes to the document are approved, they are visible to all users. You have the following options when checking in a document:

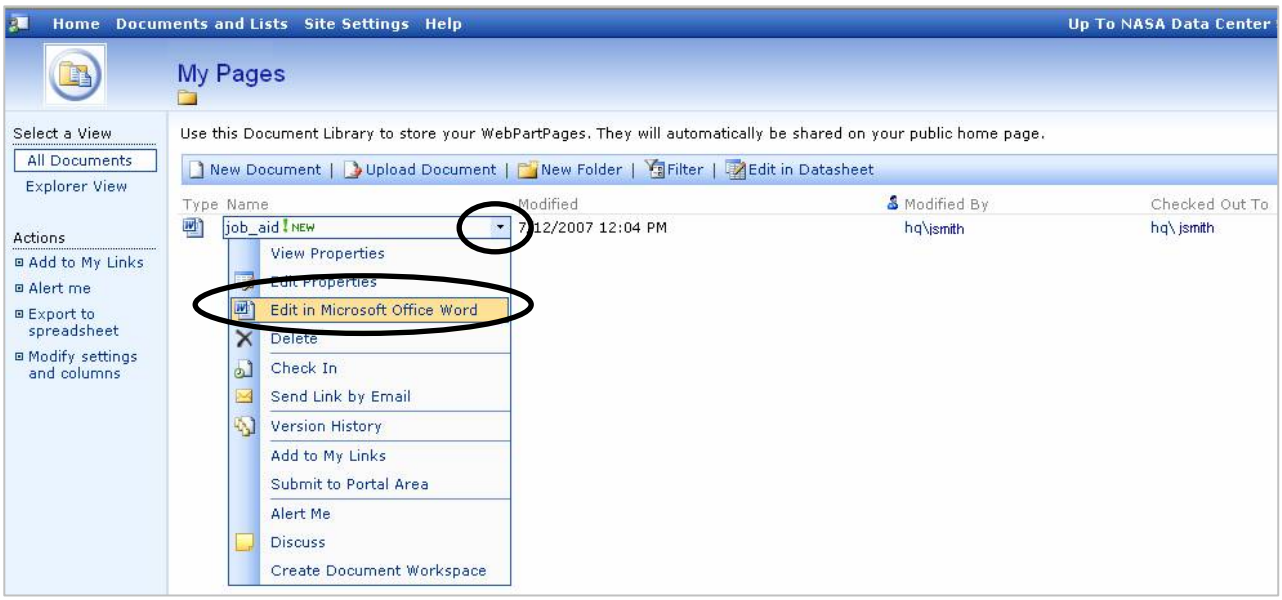
- Check in the document
- Check in saved changes to the document, but keep the document checked out
- Discard changes and undo check out

9.2.3 Edit a Document

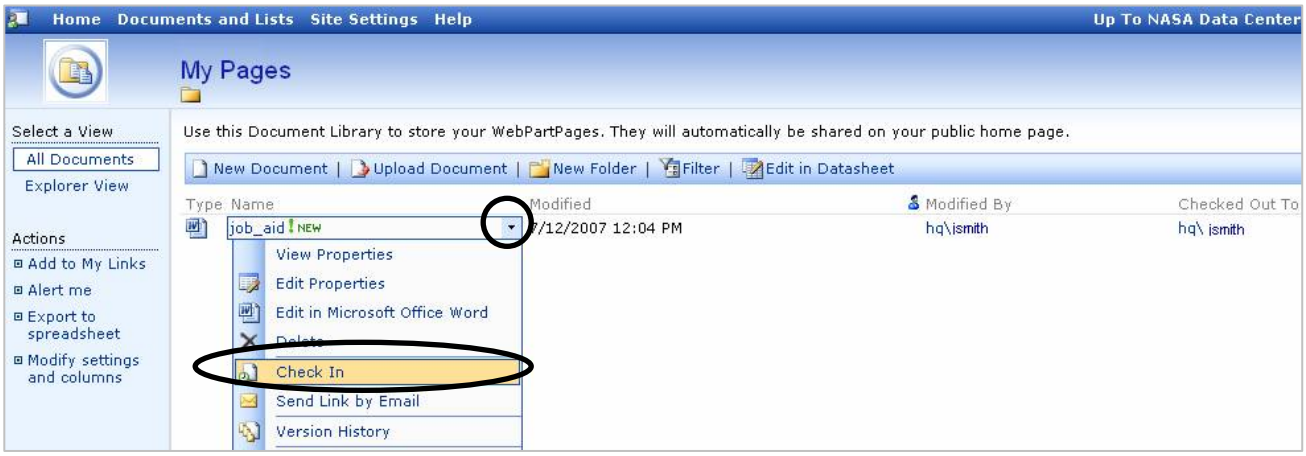
1. Locate the document to be edited.
2. Point your mouse at the document name.
3. Click the arrow icon, and click **"Check Out"**.



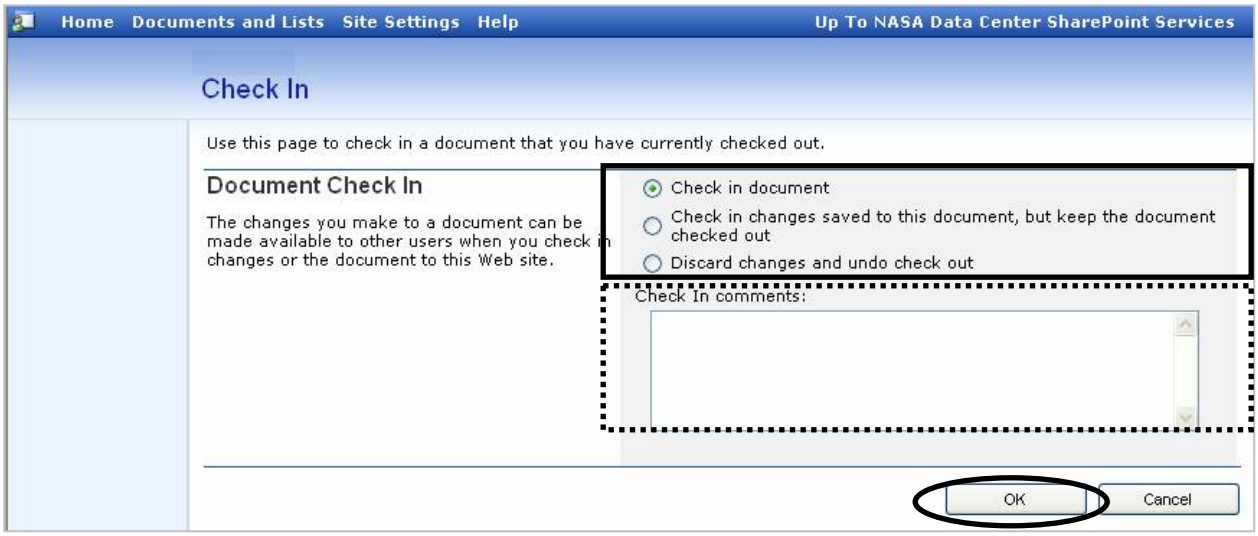
4. Point your mouse at the document name.
5. Click the arrow icon and then click "**Edit in Microsoft Office Word**".



6. Make the necessary edits, click **"Save As"**. In the **"File name:"** field, name the document.
7. Click **"Save"**.
8. Return to the document library.
9. Point your mouse at the document name; click the arrow icon and then click **"Check In"**.



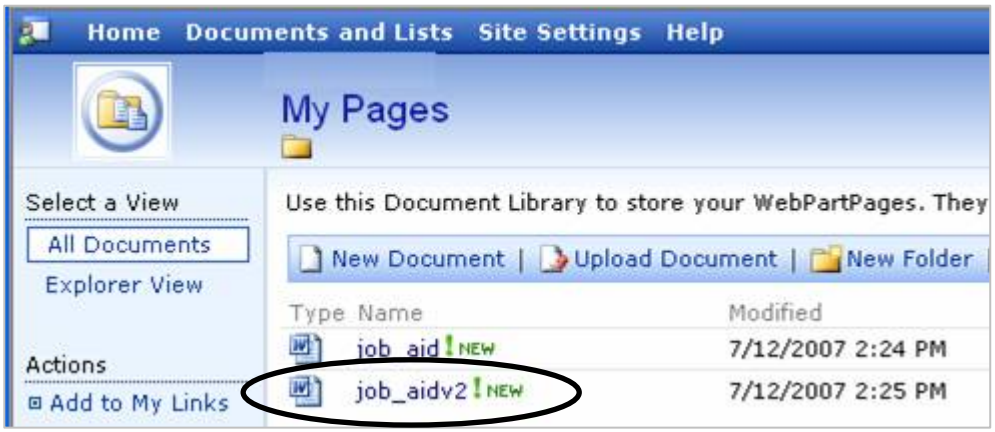
10. Select the appropriate **"Document Check In"** option.
11. Enter any comments in the **"Check In comments:**" field.
12. Click **"OK"**.



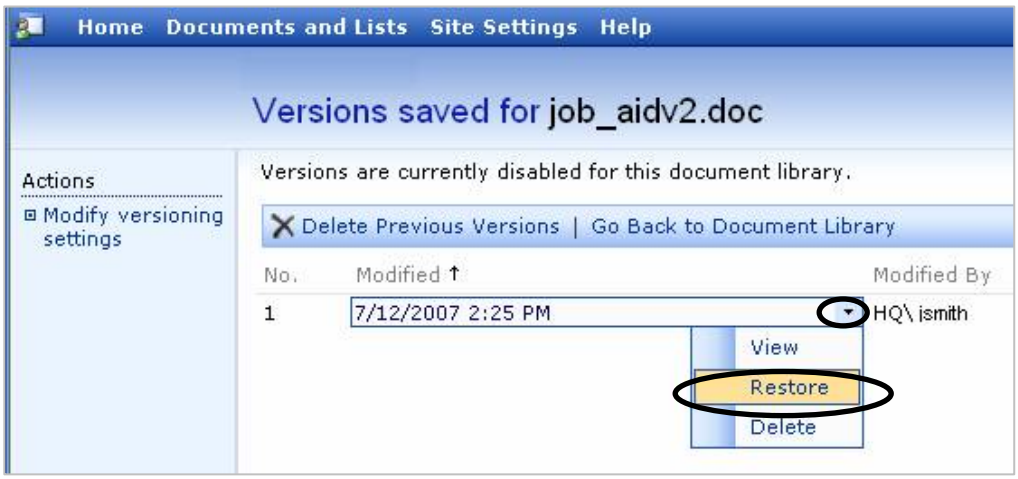
9.2.4 Restore a Document to a Previous Version

1. Point your mouse at the document name. **Note:** Document must be checked out for the **"Version History"** menu to display.
2. Click the arrow icon and then click **"Version History"**.

3. Select the version to be restored.



4. Click the arrow icon and then click **"Restore"**.



5. When prompted to confirm that you want to replace the current version of the file with the previous version, click **"OK"**.

10 WebEx

WebEx is a Virtual Team Meeting (VTM) Collaboration tool that allows users to host and participate in online virtual meetings. Usually, one person hosts a meeting and all other participants attend. Information displayed on the host computer is visible to the attendees.

10.1 Setting up Meeting Manager on Your Computer

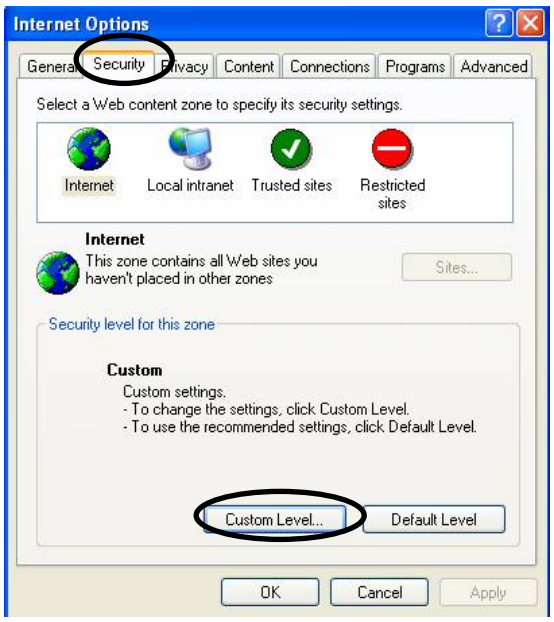
Check the Web browser's settings to see if they are correctly configured. Set up the Web browser using the following instructions.

Note: If the browser is not configured properly, you may encounter problems when setting up Meeting Manager.

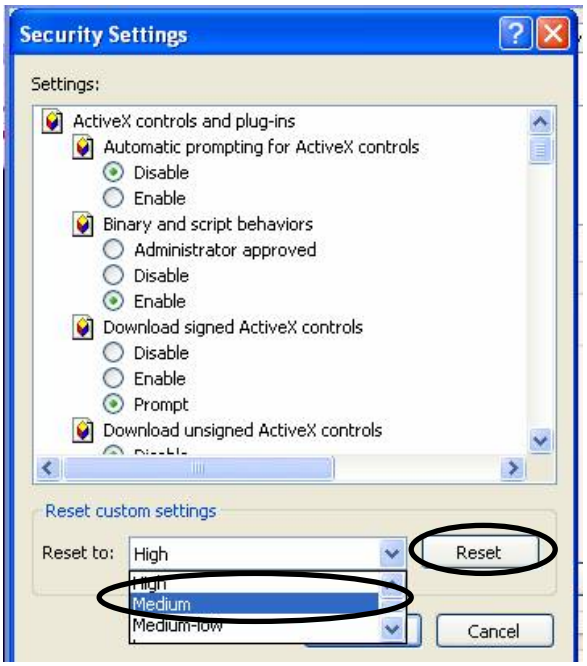
10.1.1 Setting up Internet Explorer 6.x

1. From the Internet Explorer toolbar, select Tools>Internet Options…

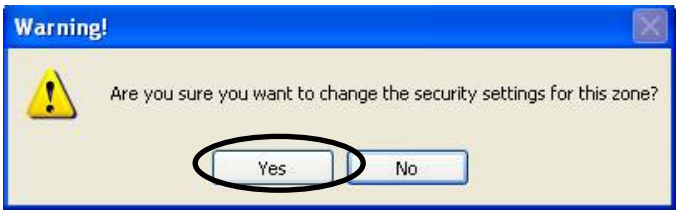
2. The Internet Options dialog box appears.
3. Click the "**Security**" tab.
4. Click "**Custom Level…**".



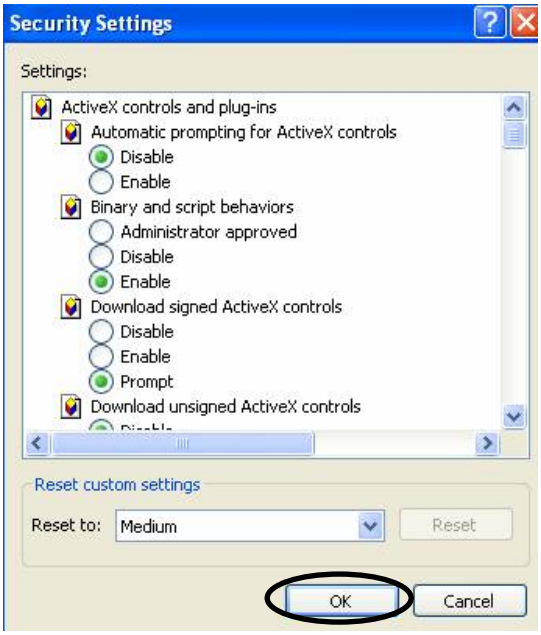
5. The **"Security Settings"** window displays.
6. From the **"Reset to:"** drop-down menu, select **"Medium"**. Click "**Reset**".



7. A **"Warning!"** message will display. Click **"Yes"**.



8. Click "**OK"** to return to the "Security" tab.

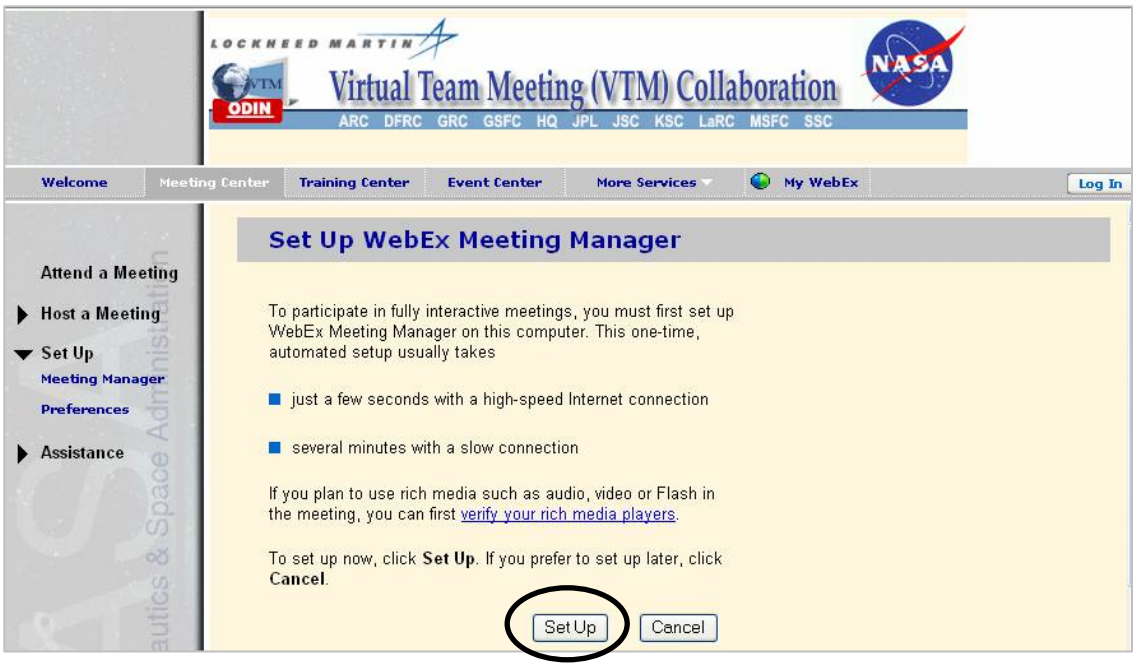


- The minimum system requirements for installing **"Meeting Manager"** on a Windows/PC are:
  - Microsoft Windows 98, ME (Millennium Edition), XP, NT, or 2000
  - Intel or AMD Processor 400 MHz
  - 128MB RAM (256MB recommended)
  - Microsoft Internet Explorer 6, Mozilla 1.7, or Firefox 1.0
  - JavaScript and cookies enabled in the browser
  - 56K or faster Internet connection
- The minimum requirements for installing **"Meeting Manager"** on a Mac OS are:
  - Mac OS 10.2.x or later
  - Safari 1.1 or Firefox 1.0
  - JavaScript and cookies enabled in the browser
  - 56K or faster Internet connection

10.1.2 Setting up Meeting Manager for Windows and Macs

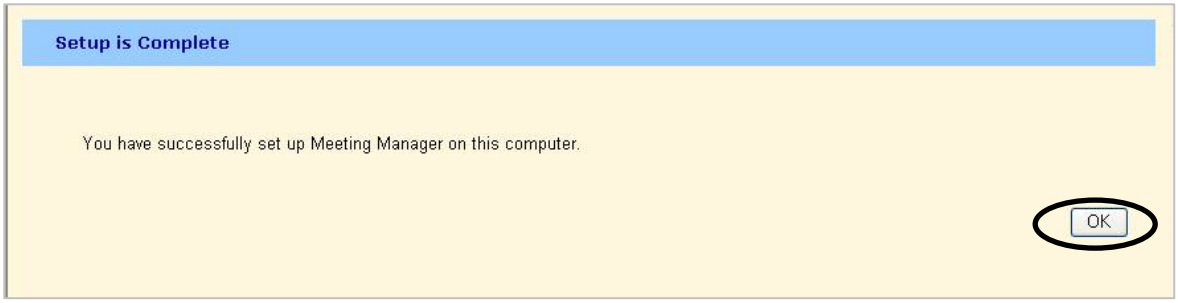
1. On the navigation bar, expand **"Set Up"**.
2. Select "**Meeting Manager"**.

3. The **"Set Up"** page displays.
4. Click "**Set Up**".



5. Click **"Install"**.

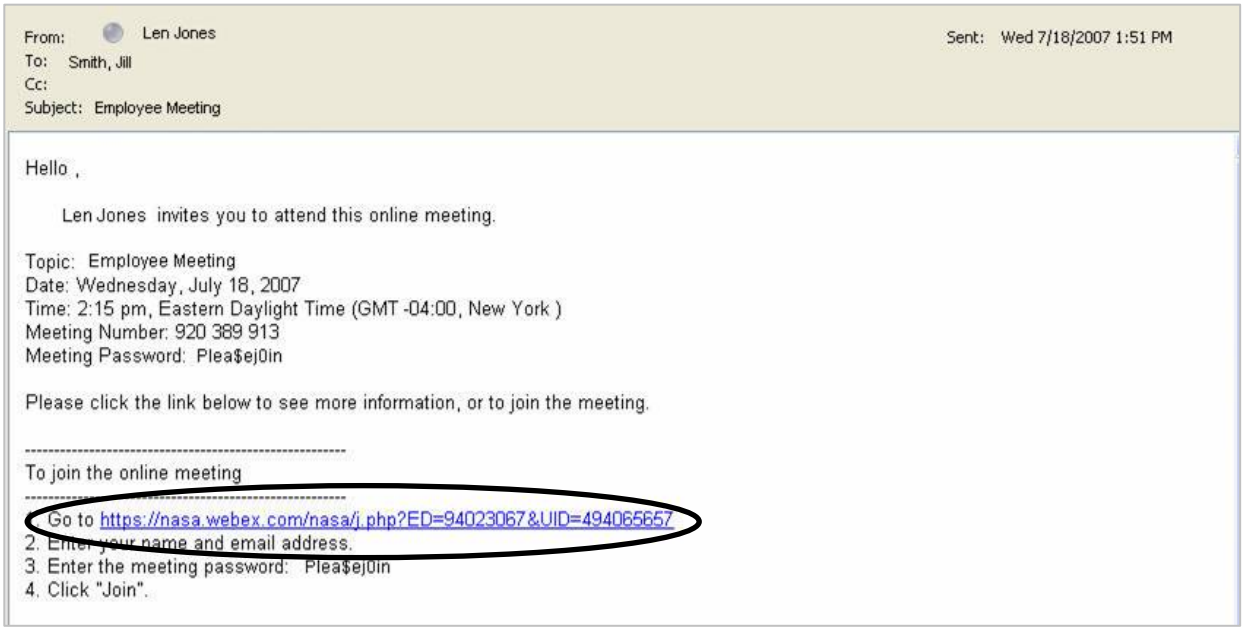
6. A **"Setup is Complete"** message displays; click **"OK"**.



10.2 Joining Meetings

If you received an e-mail invitation to a meeting, you can join the meeting by clicking a link in the invitation:

1. Open the e-mail invitation; click the provided link.



2. The **"Virtual Team Meeting (VTM) Collaboration"** page will display; enter the **"Meeting password"**.
3. Click **"OK"**.

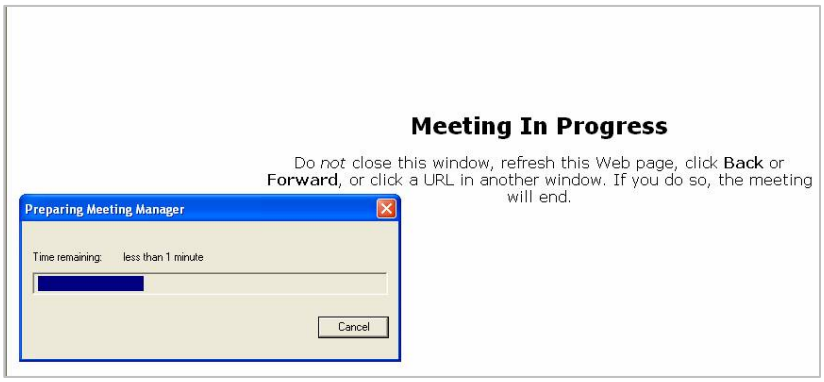
4. Select **"Join Now"**.

5. The **"Join Meeting: [Topic]"** page displays; enter the required information.

Note: If the meeting requires registration, click **"Register".** If you have not yet registered for the meeting, you must do so before you can join it.

6. Click **"OK"**.

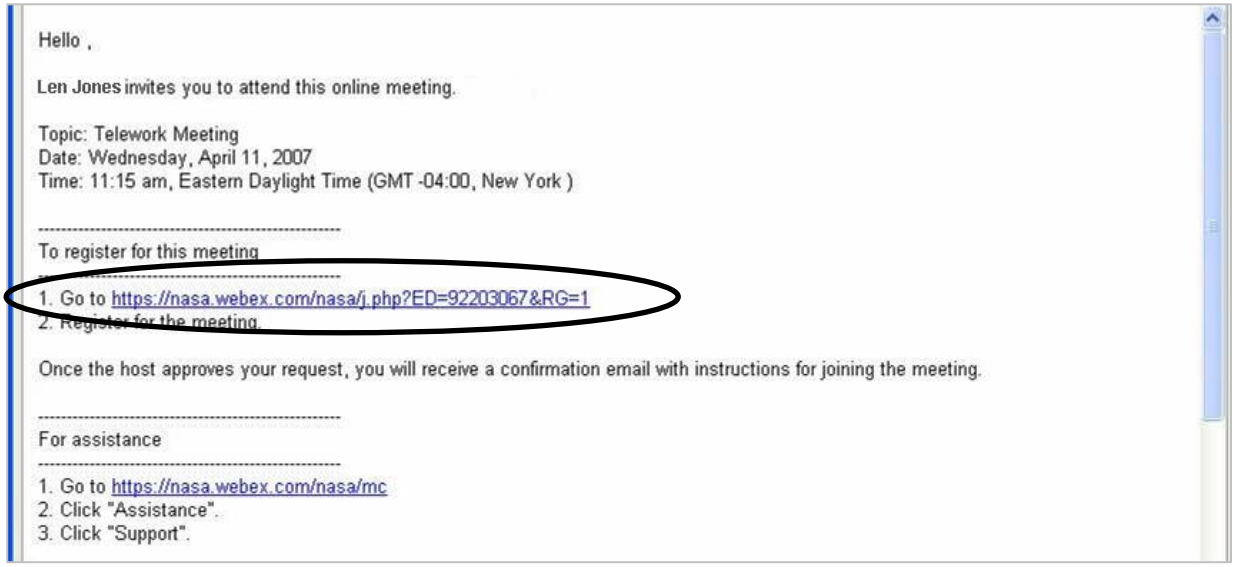
7. The **"Meeting In Progress"** window will display. **Note:** Do not close the **"Meeting In Progress"** window. If you do so, the meeting will end.



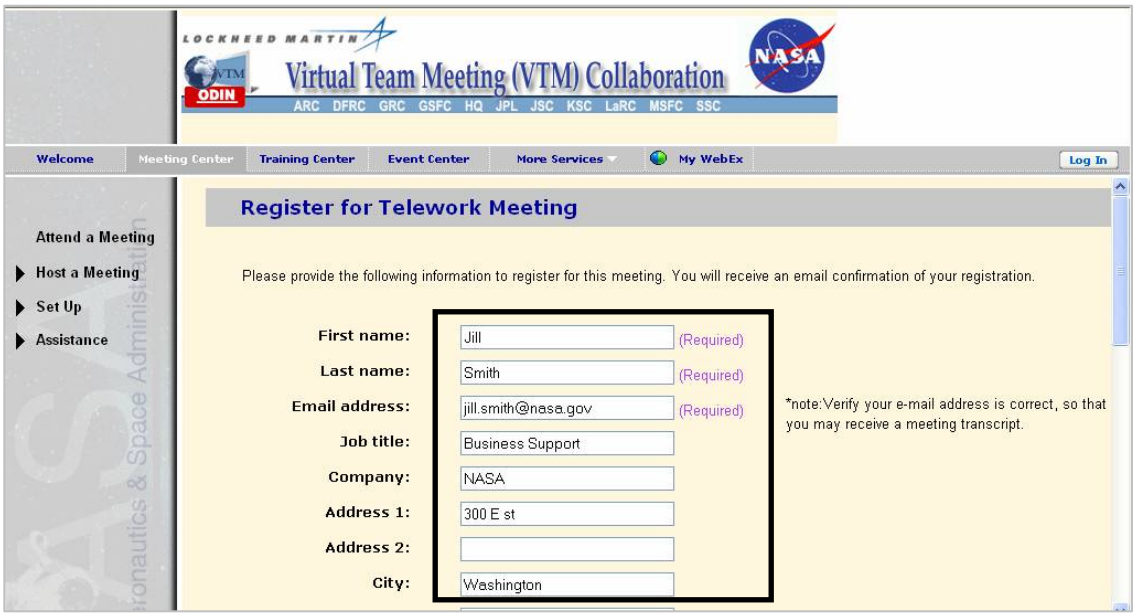
10.2.1 Registering for a Meeting from an E-mail Message

If you received an invitation for a meeting that requires registration, you can register for the meeting from the message. To register for a meeting from an invitation e-mail message:

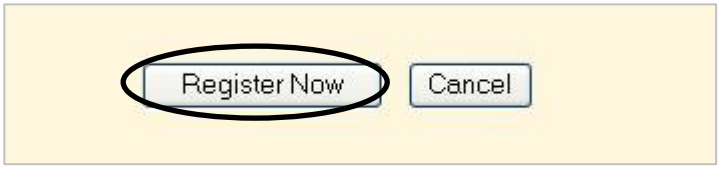
1. Open your invitation e-mail and click the link to register for the meeting.



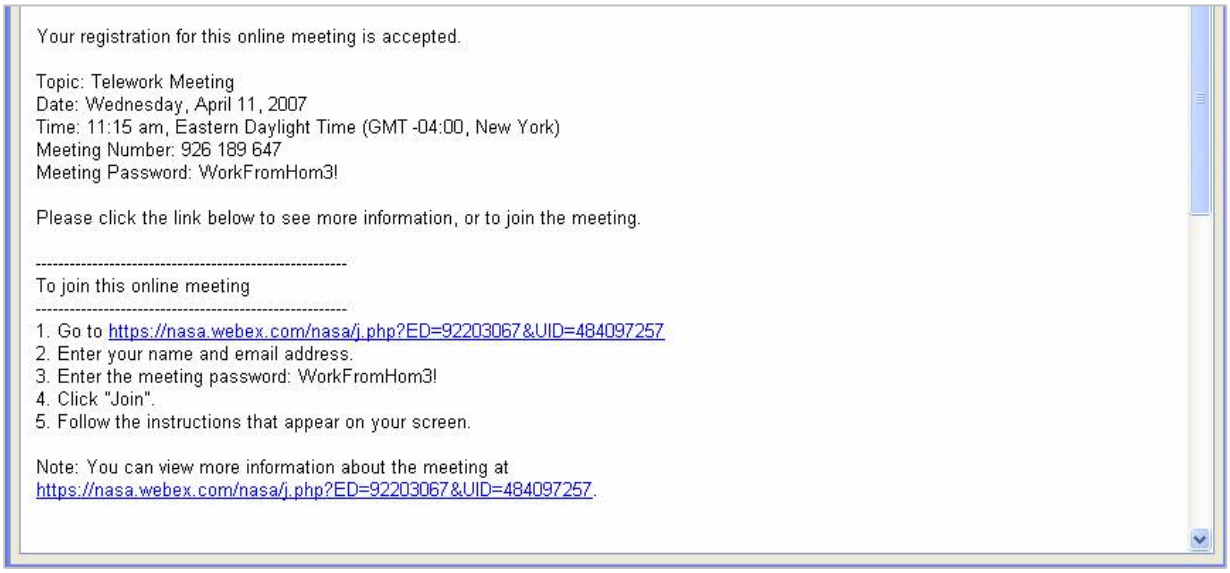
2. The **"Register for [Topic]"** page displays; enter the required information.



3. Click **"Register Now"**.



4. Once the host approves the registration, you will receive a registration confirmation e-mail message; you can then join the meeting once it starts. If the meeting is already in progress, and the host has chosen to approve all registration requests automatically, you will join the meeting immediately.



Your registration for this online meeting is accepted.

Topic: Telework Meeting
Date: Wednesday, April 11, 2007
Time: 11:15 am, Eastern Daylight Time (GMT -04:00, New York)
Meeting Number: 926 189 647
Meeting Password: WorkFromHom3!

Please click the link below to see more information, or to join the meeting.

To join this online meeting
---
1. Go to https://nasa.webex.com/nasa/j.php?ED=92203067&UID=484097257
2. Enter your name and email address.
3. Enter the meeting password: WorkFromHom3!
4. Click "Join".
5. Follow the instructions that appear on your screen.

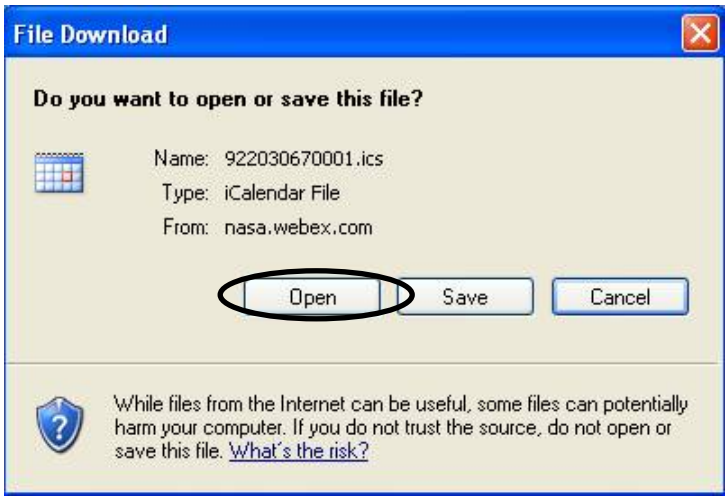
Note: You can view more information about the meeting at
https://nasa.webex.com/nasa/j.php?ED=92203067&UID=484097257.

10.2.2 Adding a Meeting to Your Calendar Program

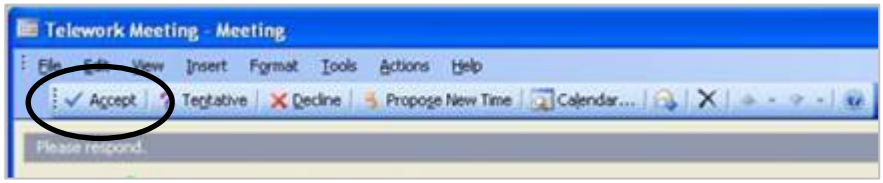
You can add a scheduled meeting to your calendar program if your calendar program supports the **"iCalendar"** standard.

1. From the **"Meeting Information"** page, click **"Add to My Calendar"**.

2. If a **"File Download"** window appears, click **"Open"**.



3. A meeting item opens in your calendar program; click **"✓Accept"** to add to your calendar.



Note: If the host cancels the meeting, the cancellation e-mail message that you receive contains a link to remove the meeting from your calendar.

This page was intentionally left blank.