

SAO Remote Access POLICY

FINAL

Contents

PURPOSE.....	4
SCOPE	4
POLICY	4
AUTHORIZATION	4
PERMITTED FORMS OF REMOTE ACCESS.....	5
REMOTE ACCESS USER DEVICES.....	5
OPTION ONE: SAO-OWNED PC.....	5
OPTION TWO: EMPLOYEE-OWNED PCS	5
SECURITY	5
GENERAL PROTECTION GUIDELINES	6
TERMINATION OF REMOTE ACCESS RIGHTS	7
EXCEPTION.....	8
COMPLIANCE	8
APPENDIX A – REMOTE ACCESS CERTIFICATION FORM	10
APPENDIX B - SAO REMOTE ACCESS PROCEDURES.....	13
APPENDIX C - REQUEST FOR SECURITY POLICY/PROCEDURES EXCEPTION	23

Version

Version	Date	Revision / Description	SAO Approval
1	3/11/2009	Original Document	Roger Smith
2	7/01/2013	Update	Roderick L Wright Theinraja Raja

STATE ACCOUNTING OFFICE
Security Policy
Remote Access Policy

EFFECTIVE DATE: *June 25, 2013*

RELEASE DATE: *July 1, 2013*

REFERENCE: *GTA Secure Remote Access (SS-08-038)*
GTA Teleworking and Remote Access (SS-08-037)
GTA Wireless and Mobile Computing (SS-08-039)

PURPOSE

The purpose of this policy is to protect SAO internal information resources from the risks associated with remote access. This policy document outlines the policy and procedures for remotely connecting to SAO LAN. This procedure has been put in place to improve security in accordance with Georgia Technology Authority (GTA) policies and applicable State and Federal laws. All remote access should use the following procedure only. No other mode of remote access is approved except what is detailed in this document. Any exceptions to use other means of connectivity to the SAO LAN have to be approved by the SAO Information Security Officer. If you have any questions or concerns, please address them to your supervisor.

SCOPE

This policy applies to all SAO employees, including contractors, vendors and agents who utilize SAO or personally-owned computers to remotely access the SAO LAN.

Any and all work performed for SAO on said computers by any and all employees, through a remote access connection of any kind, is covered by this policy. Work can include (but is not limited to) e-mail correspondence, web browsing, Instant messaging, utilizing intranet resources, and any other SAO application used over the Internet. Remote access is defined as any connection to SAO LAN and/or other applications from off-site locations, such as the employee's home, a hotel room, airports, cafés, wireless devices, etc.

POLICY

AUTHORIZATION

Remote access must be approved in writing by the SAO Information Security Officer. Approvals are granted on an annual, per-user, per-application basis. Users may request remote access to the SAO network by completing a Remote Access Certification (RAC) form. The RAC form must be approved and signed by the employee's manager, supervisor, or department head before submission to the SAO Security department. Requests for approval and renewal will be processed and stored by the SAO Information Security Officer. RAC forms are available in **Appendix A**. Employees must complete all sections of, and sign, the RAC form prior to approval.

PERMITTED FORMS OF REMOTE ACCESS

All authorized users shall conduct remote access through the use of the SAO SSL VPN. SAO employees should use the SAO SSL VPN to connect to the SAO LAN prior to accessing SAO information technology network resources, such as computers, servers, printers, etc. Access to the VPN is authenticated, encrypted, and logged.

Use of the SAO VPN is limited to authorized individuals; including contractors, vendors and agents, to conduct work. Connecting to the SAO VPN constitutes acceptance of the **SAO Enterprise Security Policy** as well as consent to monitoring.

Please refer to **Appendix B** for details of connecting remotely to SAO LAN.

REMOTE ACCESS USER DEVICES

For those employees who have been assigned authorized remote access privileges, SAO offers two options of types of remote access user devices authorized for use. The decision regarding which option to use will be discussed collaboratively between the employee and his/her supervisor.

OPTION ONE: SAO-OWNED PC

Remote access user devices in this category are owned, configured, and managed by SAO.

OPTION TWO: EMPLOYEE-OWNED PCS

Devices in this category are owned by the remote access user who is ultimately responsible for securing them and maintaining their security. Financial reimbursement for remote access devices are not the responsibility of the SAO.

SECURITY

There are many threats to remote access user devices. These threats are posed by people with many different motivations, including causing mischief and disruption, and committing identity theft and other forms of fraud. This section helps identify ways SAO remote access users can increase their devices' security to provide better protection against these threats.

Employees must review the following policies and general protection guidelines for details of protecting information when accessing the SAO network via remote access methods, and acceptable use of SAO's network:

- SAO Enterprise Security Policy (In draft expected completion October 2013)
- Appropriate Use and Monitoring Policy
- Telework Policy
- Remote Access Policy

GENERAL PROTECTION GUIDELINES

Personal equipment that is used to connect to SAO's networks must meet the requirements of SAO-owned equipment for remote access.

The following are **requirements** for accessing SAO resources using remote access:

- **SAO Remote Access Certification (RAC) form**
All authorized remote access personnel shall complete the SAO RAC form (see Appendix A) and have it signed by their supervisors and submitted to SAO Security for final approval. SAO Security will maintain the RAC form for a period of 1 year post termination of employment.
- **Password Security**
At no time should any SAO employee provide their login or email password to anyone, not even family members.
- **Antivirus Software**
All hosts that connect to the SAO LAN via remote access technologies must use the most up-to-date anti-virus software. This includes personal computers.
- **Security Updates (Patches)**
All hosts that are connected to SAO LAN via remote access technologies must have current operating system security patches installed.
- **Email Security**
SAO employees and contractors with remote access privileges to SAO's network must not use non-SAO email accounts (i.e., Hotmail, Yahoo, AOL), or other external resources to conduct SAO business, thereby ensuring that official business is never confused with personal business.
- **Physical Security**
All SAO issued laptops shall be physically secured by using cable locks or other deterrents to theft. This is most important for laptops in untrusted external environments, but is relevant for any environment, including home offices.

- **Prevention of Data Loss**

All SAO issued laptops that are taken off site will have the following security configured, to prevent data loss in the event of theft.

- The hardware password will be enabled if available.
- **Encrypting Data at Rest**- All SAO data on the laptop shall be encrypted using appropriate encryption software post the Windows 7 migration in 2013.

Note: If your Laptop is lost, stolen, or broken notify the Consolidated Service Desk (CSD) at 1-877-482-3233.

- **Split - Tunneling**

SAO employees and contractors with remote access privileges must ensure that their SAO-owned or personal computer or workstation, which is remotely connected to SAO's network, is not connected to any other network at the same time, with the exception of personal networks that are under the complete control of the user.

- **Wireless Access (Wi-Fi)**

Where the SAO LAN is accessed remotely via wireless appropriate wireless security standards will be used. Wi-Fi Protected Access (WPA) or greater will be used where it is available. At minimum Wired Equivalency Protocol (WEP) will be used on Wi-Fi connections. Do not connect using unencrypted Wi-Fi networks.

TERMINATION OF REMOTE ACCESS RIGHTS

A users remote access rights will be terminated:

- Upon expiry for time limited rights
- Upon separation from the SAO, in all cases
- Upon termination of an contractual relationship
- In the event of violation of this or other SAO policies regarding information technology

EXCEPTION

Exceptions to a policy or standard must be approved by the SAO Information Security Officer. The Request for Security Policy/Procedures Exception form can be found in **Appendix C**. In each case, the agency or vendor must include such items as the need for the exception, the scope and extent of the exception, the safeguards to be implemented to mitigate risks, specific timeframe for the exception, organization requesting the exception, and the management approval. Denials of requests for exceptions may be appealed to the State Accounting Officer.

COMPLIANCE

Violation of this policy may result in disciplinary action, which may include termination for employees and temporaries; a termination of employment relations in the case of contractors or consultants. Additionally, individuals are subject to loss of SAO Information Resources access privileges, and to civil and criminal prosecution.

APPENDIX A

FENVAL

APPENDIX A – REMOTE ACCESS CERTIFICATION FORM

<p>State Accounting Office TeamWorks Security</p> <h2 style="text-align: center;">Remote Access Certification Form</h2> <p style="text-align: center;">Completed forms are to be returned to TeamsWorks Security. Forms can be emailed to pssecadm@sao.ga.gov.</p>					
Request Type:	New:		Change:		Delete:
If termination or transfer, please provide the Effective Date:				Effective Time:	
User/Contact Information					
User's name (First Mi. Last)					
User's Email					
USERID:					
Work Number:		Alternate Number			
User Status:		SAO User: <input type="checkbox"/>		Contractor: <input type="checkbox"/>	
Computer:		SAO-Owned: <input type="checkbox"/>		Employee-Owned <input type="checkbox"/>	
<hr style="border: 0.5px solid black;"/> Decal #					
Additionally, please identify the following about your home computer setup					
Windows Version:	Windows 7 <input type="checkbox"/>	Windows 2000 <input type="checkbox"/>	Windows XP <input type="checkbox"/>	Other <input type="checkbox"/>	
Firewall Installed:	Yes <input type="checkbox"/> No <input type="checkbox"/>		Software: Yes <input type="checkbox"/> No <input type="checkbox"/>	Hardware: Yes <input type="checkbox"/> No <input type="checkbox"/>	
Do you use virus protection software?	Yes <input type="checkbox"/> No <input type="checkbox"/>		If yes, what software and version		
Is your virus protection software maintained? (Automatic virus definition file updates)				Yes <input type="checkbox"/> No <input type="checkbox"/>	
Are you running a local network? Yes <input type="checkbox"/> No <input type="checkbox"/>			If yes, what IP address scheme are you using (ie. 192.168.x.x-255)?		

Do you have Broadband internet access? Yes <input type="checkbox"/> No <input type="checkbox"/> Note: Dial up (>1.5 Mbps) access is not permitted.	
By signing below, I signify that I have read and understand that I am subject to all the provisions of: <ul style="list-style-type: none"> SAO Enterprise Security Policy Appropriate Use and Monitoring Policy Telework Policy Remote Access Policy 	
I understand that every user is responsible for systems security to the degree that his or her job requires the use of information and associated systems. All users are responsible for using information resources only for the purposes for which they are intended, to comply with all controls established by information resource owners and custodians and for protecting sensitive information against unauthorized disclosure, theft, damage or destruction. I also understand that it is my responsibility to protect all of my passwords from being disclosed and to refuse to use any other user's password. All passwords must be changed at least every sixty (60) days. Users must take steps to ensure physical security and protection from theft, damage or unauthorized use. Users are required to terminate connections to the SAO network when workstations are unattended.	
Users's Signature: _____ Date: _____	
Managerial Approval	
Department Name:	
Approving Manager's Name	Phone Number:
SAO Security	
Received by:	Date:
<input type="checkbox"/> Approved <input type="checkbox"/> Rejected By:	Date:
Contractor Information	
Project Manager's Name:	Phone Number:
PM Email:	
PM Signature:	
Company:	
Project Name:	
Start Date:	End Date:
Purpose:	
Comments	

APPENDIX B

FENVAL

APPENDIX B - SAO REMOTE ACCESS PROCEDURES

SAO Remote Access: Procedures for connection to the SAO LAN

PART I – Prepare your workstation

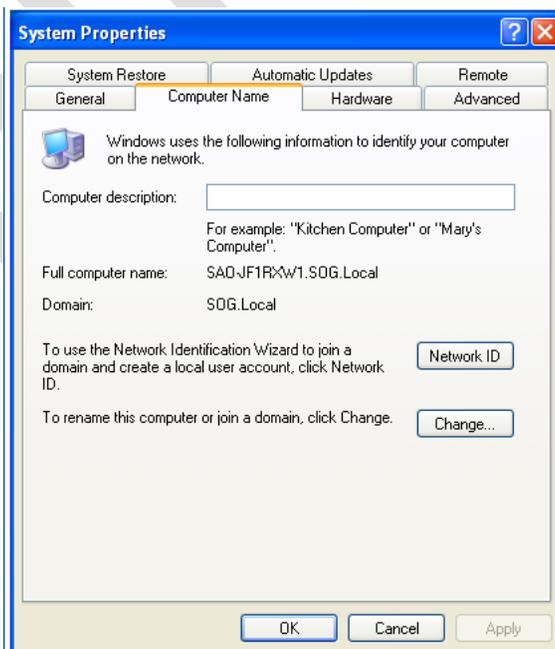
Remote Access How to:

When you want to access your workstation at your desk from a remote location, connect to Juniper SSL VPN first and then make a “Remote Desktop” connection to your office workstation.

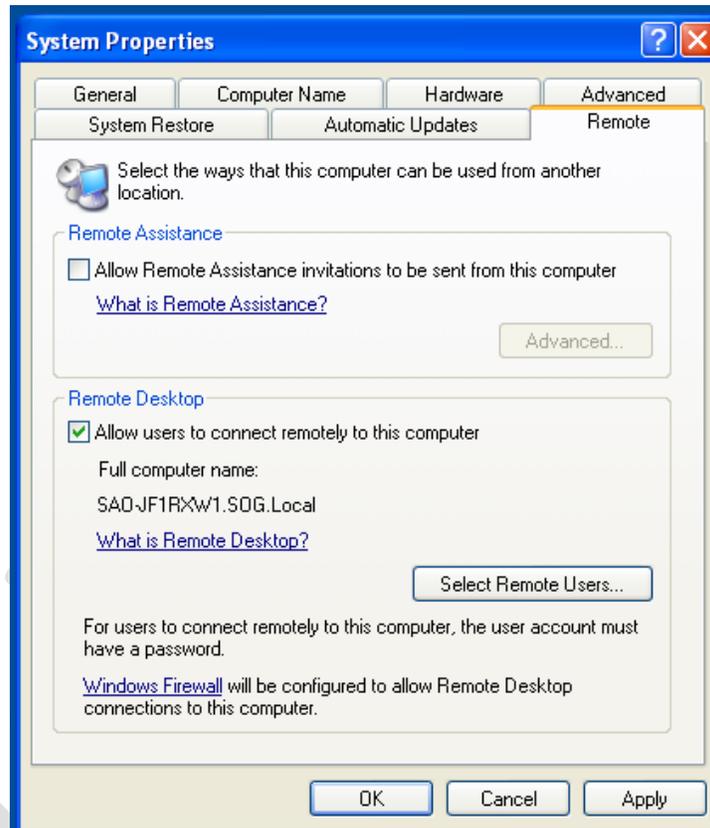
REMINDER: Get all required information and prepare your workstation for remote access **BEFORE YOU LEAVE OFFICE.**

To make this happen, you will need to

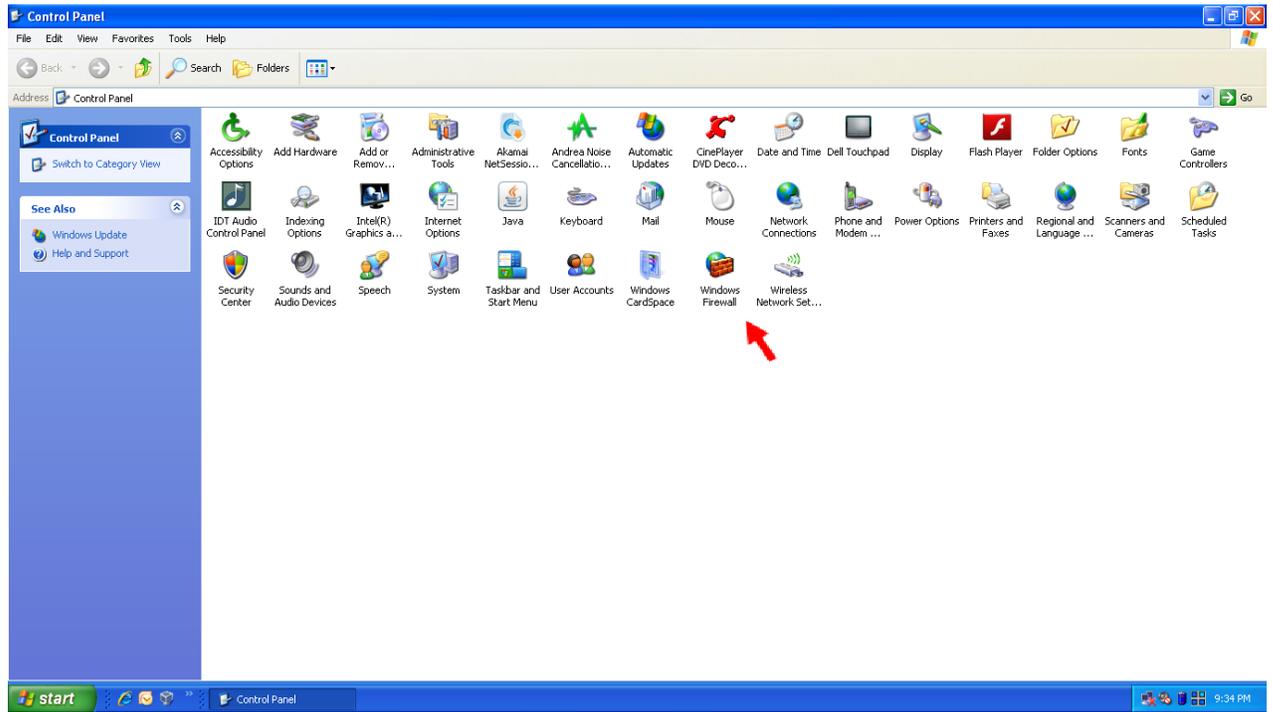
1. Have your office workstation running and in ‘locked’ status
2. Know your computer’s name
 - a. To get your Computer’s Name follow this procedure:
 - i. Right click on “My Computer” on your desktop and select ‘Properties’.
 - ii. Select “Computer name” tab.
 - iii. Your computer name will be listed against “Full Computer Name”, “**sao-xxxxxxx.sog.local**”.

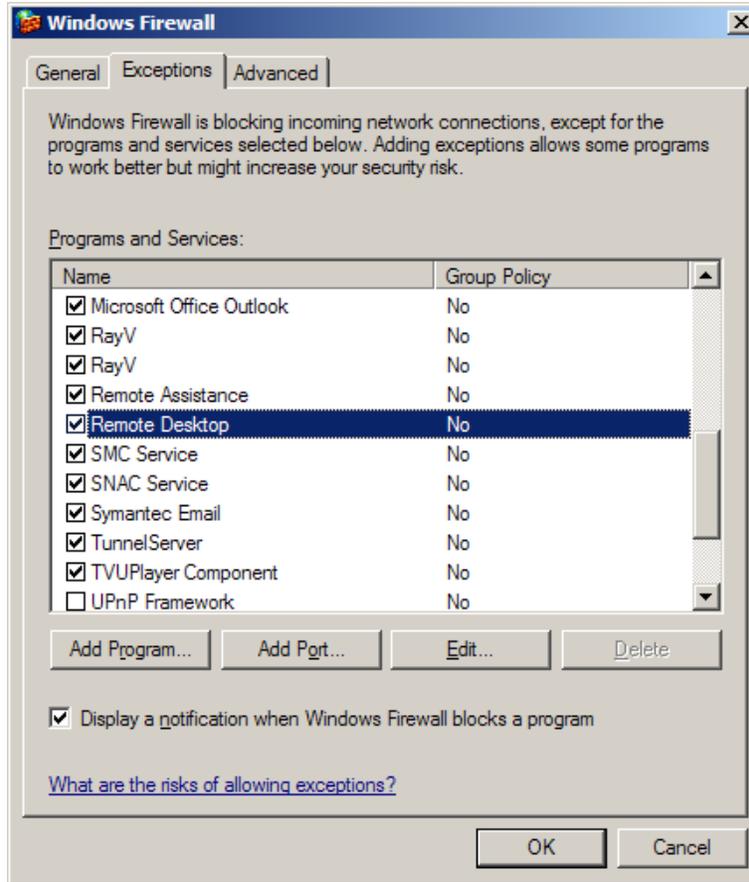


3. Have "Remote Access" enabled in your office workstation
 - a. To enable Remote Access follow this procedure:
 - i. Right click on "My Computer" on your desktop and select 'Properties'.
 - ii. Click on "Remote" tab.
 - iii. In the bottom section "Remote Desktop", check the box "Allow users to connect remotely to this computer".
 - iv. Select OK to save



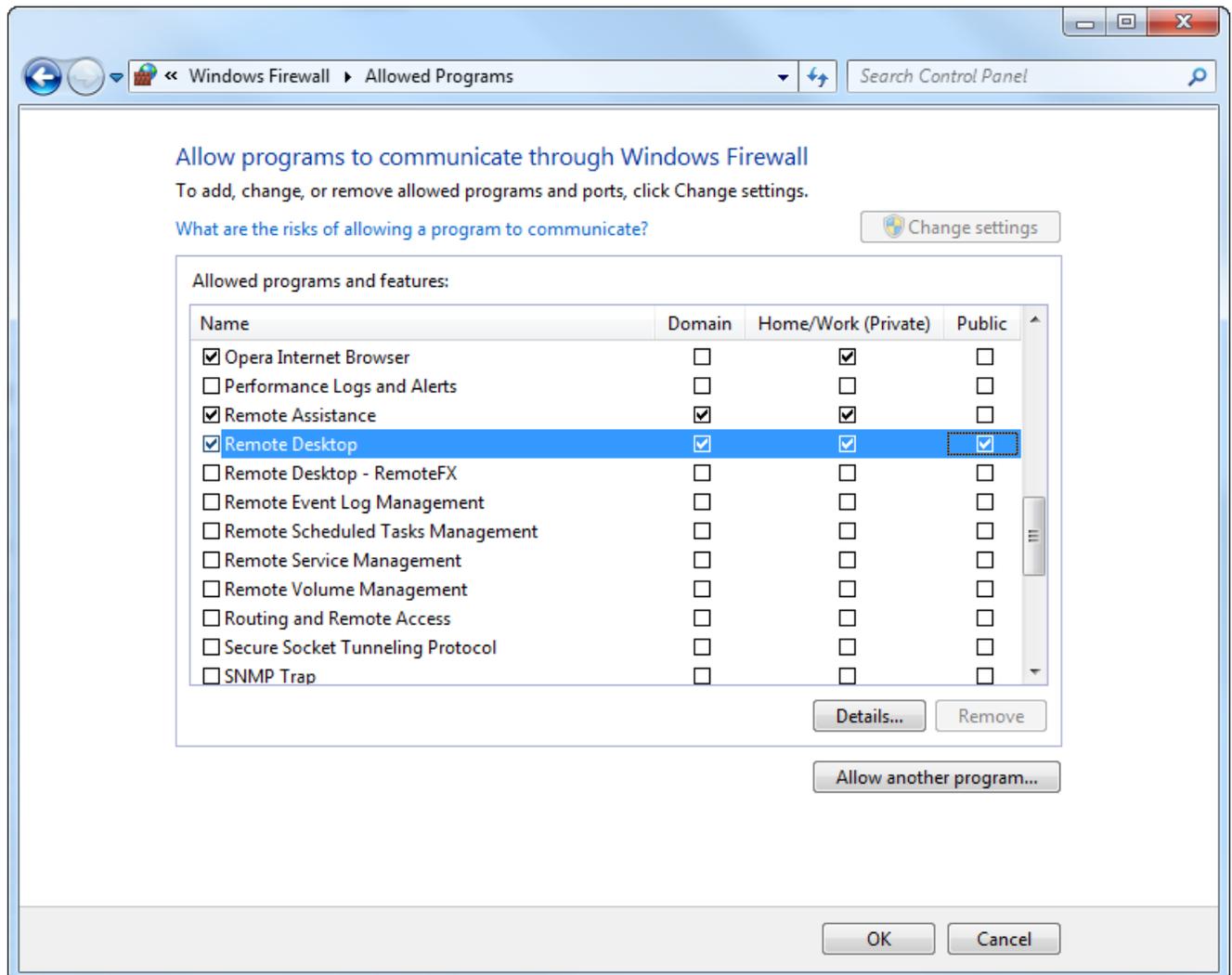
4. Configure Windows Firewall to Enable Remote Desktop Access:
 - a. **For Windows XP Users**
 - i. Select "Start" | "Settings" | "control Panel"
 - ii. Double-click "Windows Firewall"
 - iii. Select the Radio Button "On (Recommended)"
 - iv. Click on "Exceptions" Tab"
 - v. Make sure "Remote Desktop" is CHECKED. (see screenshot below)
 - vi. Click "OK" to save the settings





b. For Windows 7 Users:

- i. Select "Start" | "control Panel"
- ii. Click on "System and Security"
- iii. Click on "Windows Firewall"
- iv. Click on "Allow a program or feature through Windows Firewall"
- v. Make sure "Remote Desktop" is CHECKED and all three boxes ('Domain', 'Home/Work (Private)' and 'Public' are checked. (see screenshot below)
- vi. Click "OK" to save the settings



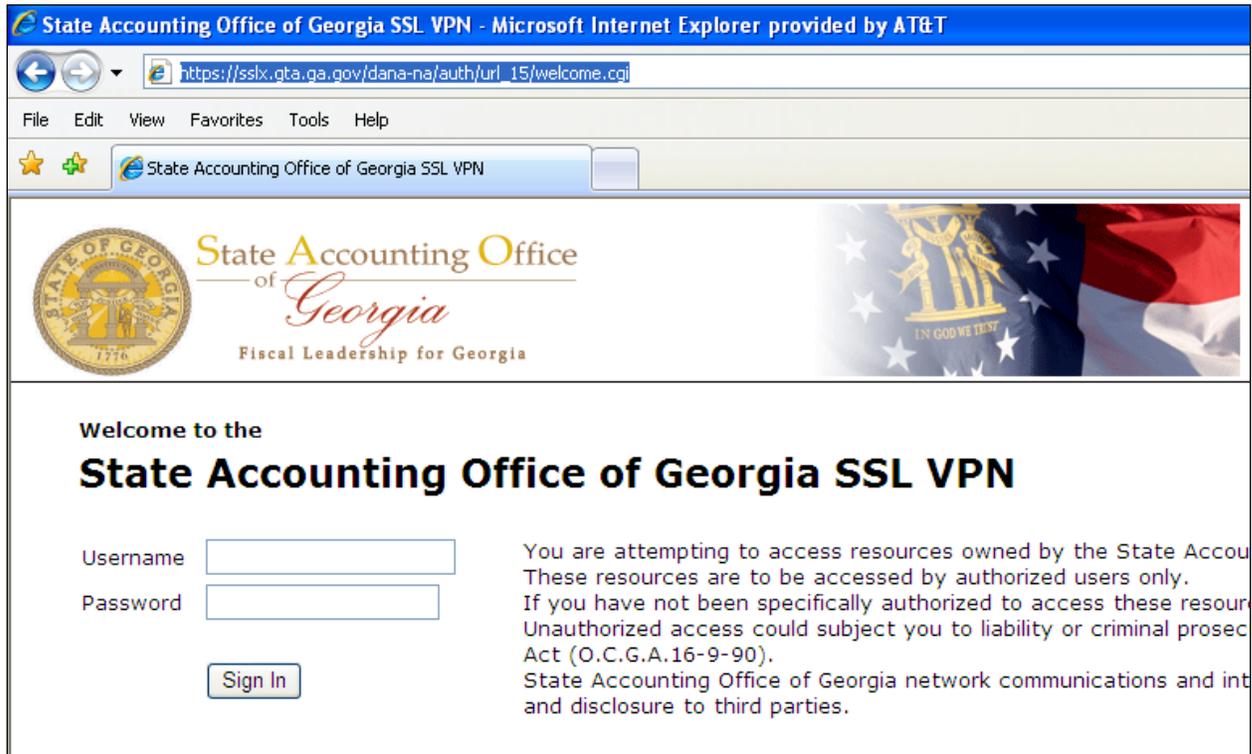
PART II - Connect to Juniper SSL VPN (Laptop or Desktop):

URLs To Use for Remote Access to SAO LAN:

URL to Juniper SSL VPN access – <https://sslx.gta.ga.gov/sao>
(If you bookmark, use above URL not any extensions of it)

SAO remote access screen

Your Juniper remote access sign-on screen is shown below.



State Accounting Office of Georgia SSL VPN - Microsoft Internet Explorer provided by AT&T

https://sslx.gta.ga.gov/dana-na/auth/url_15/welcome.cgi

File Edit View Favorites Tools Help

State Accounting Office of Georgia SSL VPN

 State Accounting Office
of Georgia
Fiscal Leadership for Georgia

IN GOD WE TRUST

Welcome to the
State Accounting Office of Georgia SSL VPN

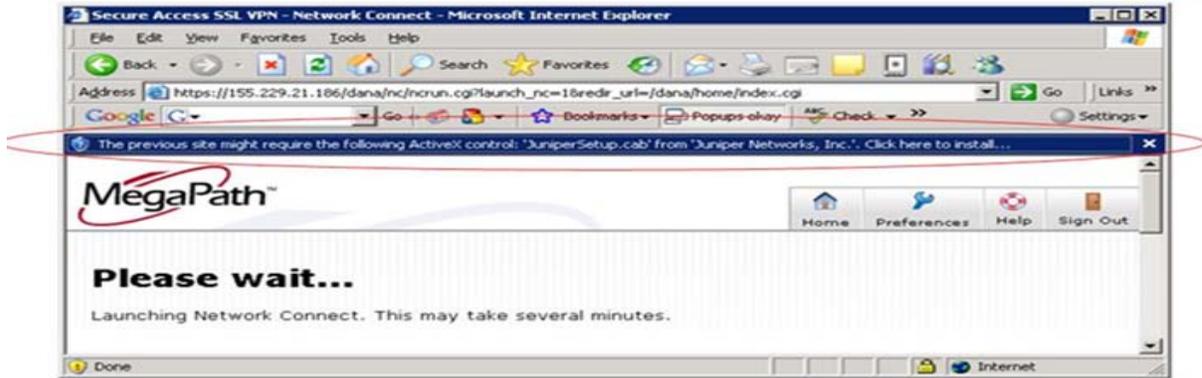
Username

Password

You are attempting to access resources owned by the State Account...
These resources are to be accessed by authorized users only.
If you have not been specifically authorized to access these resour...
Unauthorized access could subject you to liability or criminal prosec...
Act (O.C.G.A.16-9-90).
State Accounting Office of Georgia network communications and int...
and disclosure to third parties.

Use your SAO DOMAIN credentials to get authenticated.

After Successful authentication, **on first use only**, you will be required to install any necessary Juniper components. If you see any of these messages, click 'Yes, and 'Install' to be able to use SSL VPN.



Remote access screen

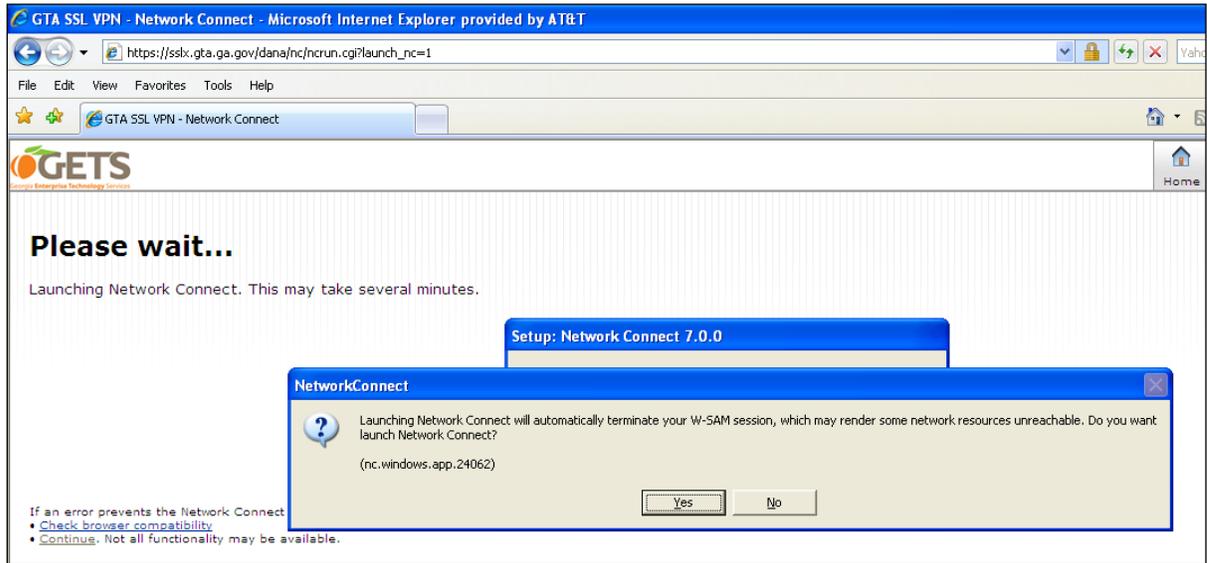
You will see the following screen when you log on. (You may see many different applications listed)

Click on “Start” button against the “Network Connect” option under “Client Application Sessions”.

Note: Do not use any other links from this page.

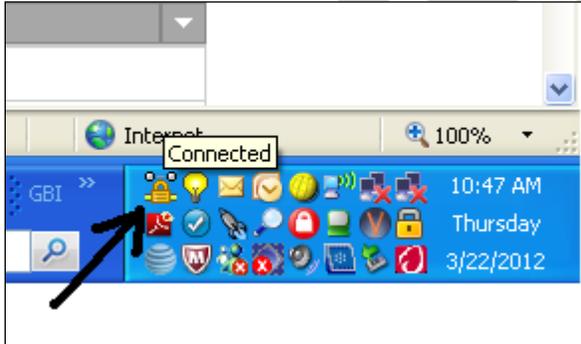


The Windows Secure Application Manager (WSAM) option runs automatically for now. Select “Yes” to stop it and continue with Network Connect.



What to look for once you've selected Network Connect

If Network Connect is running, you should see a new icon (see below) in the system tray at the bottom of your screen.



At this time, you are successfully connected to SSL VPN session

Connecting to your SAO Workstation:

In order to connect to an SAO computer using Remote Desktop, you must first establish a VPN connection to the SAO network. Otherwise your attempts to connect will be blocked by the enterprise firewall. To connect to your SAO workstation from a remote location, follow the procedures below.

From your remote computer:

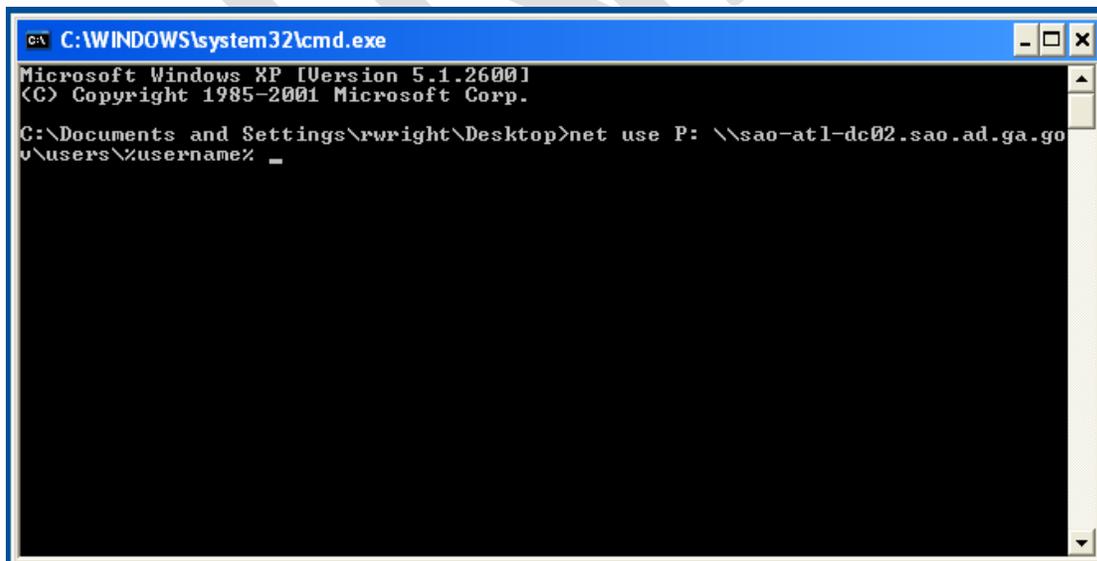
1. Start “Remote Desktop Connection” from your workstation from “Start | Programs | Accessories” OR whatever the path is depending the Operating system they use.
2. Enter your SAO desktop name “SAO-xxxxxxx.sog.local” from Computer, use your SOG Domain credentials and connect. You should now be connected to your workstation at the SAO office.

PART III – Mapping Network Drives (Laptop or Desktop):

Note: The drives listed below are the default drives available to SAO employees. Drive access is granted on the basis of Need-to-Know. If you have a valid need for access to a drive not listed please contact your manager and submit a GETS request for access.

Windows XP and Windows 7 support several different methods for mapping a network drive. A network drive is a file folder located on a remote computer that has been configured for sharing over the SAO [LAN](#). For simplicity follow the steps below.

1. Click **Start**, and then click **Run**.
2. In the **Open** box, type **cmd**.
3. Type **net use P: [\\sao-atl-dc02.sao.ad.ga.gov\users\%username%](#)** then press “Enter” key
4. Type **net use S: [\\sao-atl-svr02.sao.ad.ga.gov\share](#)** then press “Enter” key
5. Close the window.



```
C:\WINDOWS\system32\cmd.exe
Microsoft Windows XP [Version 5.1.2600]
(C) Copyright 1985-2001 Microsoft Corp.

C:\Documents and Settings\rwright\Desktop>net use P: \\sao-atl-dc02.sao.ad.ga.gov\users\%username% _
```

For any issues:

Call the Consolidated Service Desk (CSD) at 1-877-482-3233.

APPENDIX C

APPENDIX C - REQUEST FOR SECURITY POLICY/PROCEDURES EXCEPTION

Request for Security Policy/Procedures Exception

Instructions: Fill out all portions of the form applicable. If you require more space, please attach your responses to this form. Once finished, please send this form to the SAO Information Security Officer.

Contact Information:

Name: _____

Title/Department: _____

Email & Phone: _____

Date Submitted: _____

Security Policy or Procedure to which this exception applies:

Describe why this exception is needed (be as specific as possible):

Describe the security threats to the application/service and SAO infrastructure that this exception introduces:

Describe the total cost to comply with the security policy:

Does the application/service for which the security exception applies store, process, transmit, or use any of the following types of data in any way?

	Yes	No
Social Security Numbers		
SAO UserIDs		
Banking account or other financial account numbers and/or access codes or passwords for SAO or any other person or entity		
SAO Account Numbers, P-Card data, or other financial data of SAO		
Computer User Names and/or Passwords		
Personal contact data for, personnel, business partners, or members of the public		
Any data that SAO has otherwise classified as "Restricted" under the data handling schema		
Any data that SAO has otherwise classified as "Sensitive" under the data handling schema		

If you answered "yes" to any of the above items, please provide a brief explanation of how the data is used in the application/service:

Signature of contact