OFFICE OF INFORMATION TECHNOLOGY
Empowering Alaskans Through Technology

VPN – 2-factor

Virtual Private Network (VPN) allows authorized users to remotely connect to the State of Alaska (SOA) network to access files and resources that you cannot access when not connected to the SOA network (such as your home network). **These instructions are only for those who indicated they needed 2-factor authentication on their VPN request.**

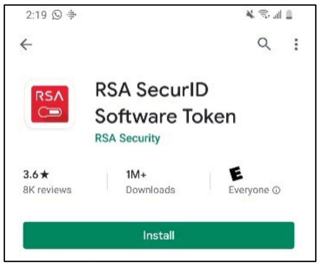
For standard VPN access, refer to: http://doa.alaska.gov/oit/docs/VPN_Access_Instructions.pdf

NOTE: When you are connected to the SOA Network using VPN, all web traffic is being diverted through the SOA Network and logged and monitored as it would be in the office environment. Avoid streaming (audio and video) while connected. Do not leave your computer unattended when VPN is active.

These instructions assume you already have VPN 2-factor permission, have VPN software installed, and have received a token. If you do not, follow the instructions here: http://oit.alaska.gov/Security/vpn

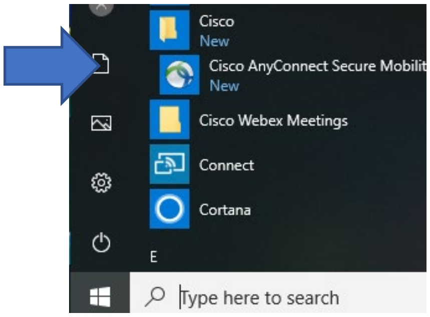
To install and set up the token:

1. Download and install the free "RSA SecurID Software Token" app from the Google Play or Apple store.
2. E-mail the token you received to yourself, and open it on your phone or device to import it to the "RSA SecurID Software Token" app.



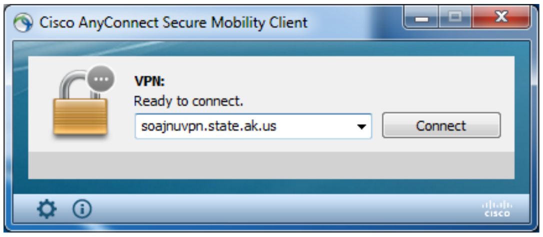
To access the SOA Network:

1. Open the Cisco AnyConnect Secure Mobility Client.



2. Type in the server name to connect to:
    a. If you are in Southeast Alaska, enter **soajnuvpn.state.ak.us**
    b. In all other areas, enter **soaancvpn.state.ak.us**

    Click "Connect".



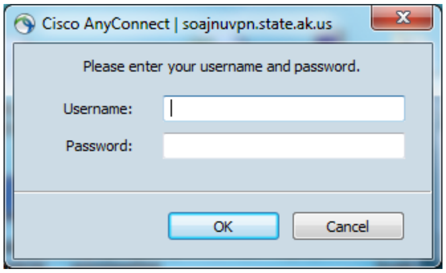
VPN:
Ready to connect.
soajnuvpn.state.ak.us

For assistance, contact oitsupport@alaska.gov
or your Department IT contact: http://oit.alaska.gov/dedpa/

OFFICE OF INFORMATION TECHNOLOGY
Empowering Alaskans Through Technology

First time logging in:

3. Enter your SOA username (for example: jbsmith) and the 6-digit passcode shown in the RSA SecurID app on your device.


Cisco AnyConnect | soajnuvpn.state.ak.us

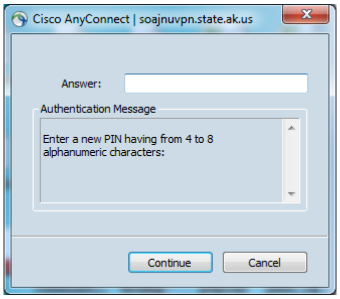
Please enter your username and password.

Username:

Password:

4. Follow the prompts to set a 4-8 character personal PIN (no spaces or special characters) and click “Continue”.

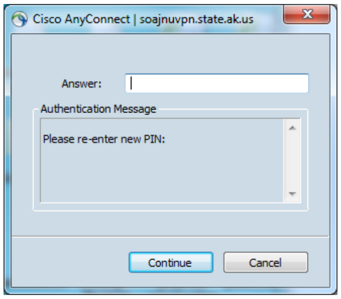
5. Re-enter your PIN for verification. Click “Continue”.


Cisco AnyConnect | soajnuvpn.state.ak.us

Answer:

Authentication Message

Enter a new PIN having from 4 to 8 alphanumeric characters:


Cisco AnyConnect | soajnuvpn.state.ak.us

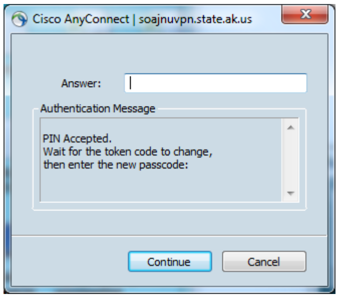
Answer:

Authentication Message

Please re-enter new PIN:

Before continuing, ensure the token has changed from last use (this may take up to 60 seconds).

Your password is now PIN+tokencode. FOR EXAMPLE: if your personal PIN was Duck9000 and the token on your device is 123456, your password is Duck9000123456.


Cisco AnyConnect | soajnuvpn.state.ak.us

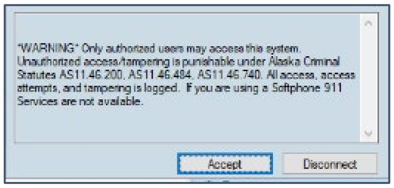
Answer:

Authentication Message

PIN Accepted.
Wait for the token code to change,
then enter the new passcode:

6. Enter your new password and click “Continue”.

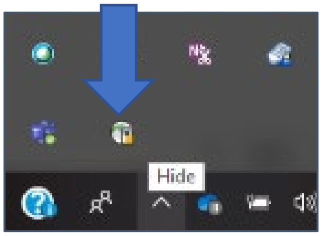
7. After you review and accept the access warning you are connected to the SOA Network and can work as if you were at your desk.

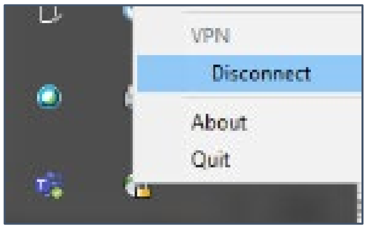

WARNING Only authorized users may access this system. Unauthorized access/tampering is punishable under Alaska Criminal Statutes AS11.46.200, AS11.46.484, AS11.46.740. All access, access attempts, and tampering is logged. If you are using a Softphone 911 Services are not available.

All future logins will require the PIN+tokencode password.

Note: If you enter the wrong password too many times, your account will be locked. Contact your IT helpdesk for assistance. Resetting your SOA password will not unlock your RSA SecureID account.

When you no longer need access to the SOA Network, be sure to disconnect from VPN by right-clicking on the Cisco icon in your system tray and selecting “Disconnect.”




VPN
Disconnect
About
Quit