AZNet II VPN Transition
Frequently Asked Questions

AZNetII

1. Why is the VPN process changing?
   The VPN platform is changing to increase security to protect the State's data and network. The dual authentication is required security enhancement.

2. Will there be additional service costs because of this change?
   There will be no additional service costs for this migration to a new platform. This change is part of the services already contracted.

3. What VPN platform does AZNet use?
   RSA. It is one of the most common platforms for duel authentication technology.

4. What is "dual authentication"?
   Dual authentication requires a user to provide two means of identification in order to use a service. The user must "know something" like a password and the user must "have something" like a uniquely created code sent using a token.

5. What new processes or procedures will affect the user?
   The user will have one additional code to enter when using the dual authentication VPN login process. The user obtains the additional code through either through a soft token (a computer, tablet or smart phone application) or through a hard token (similar to a key fob).

6. What is the difference between a hard token and a soft token?

   

   There are two kinds of SecurID tokens, hardware tokens and software tokens. Software token are applications that generate tokencodes on the smart phone or other device. Hardware tokens generate tokencodes using a built-in clock and the token's factory-encoded random key, known as the "seed." AZNet offers the Hardware tokens called keyfobs).

   

7. How do I know whether to choose a hard token or a soft token?
   Most agencies will allow for either, but if you have questions or concerns about the type of token you should choose, check with your agencies coordinator for additional information.

8. How do I find out who my agency coordinator is?
   Contact the ADOA Service Desk through an email to AZNETSUPPORTDESK@AZDOA.GOV or call 602-364-4444 Option 1.

9. Is access to BlueZone impacted?
   No. BlueZone is a web-based application that requires a VPN in order to access the mainframe systems. Users transitioning from the current ADOA VPN platform to the AZNet VPN platform will not experience any changes related to BlueZone.

10. What happens if the dual authentication fails during the process of migrating to the new platform?
    The VPN Migration team planned for this event. Both the "current" and the "new" VPN access methods will be supported during the initial migration phase. Users are asked to contact the ADOA Service Desk with issues encountered during this time frame regardless of which VPN access method is causing concern.

11. I tried to Login, but my account is blocked. Who do I contact?
    Your account will lock up after 5 failed attempts in a 15 minute period. The system will automatically reset if this happens. Wait 10 minutes and try logging in again. If you still cannot login, or you have forgotten your login or password, contact the ADOA Service Desk through an email to AZNETSUPPORTDESK@ AZDOA.GOV or call 602-364-4444 Option 1.

12. What if I forgot my PIN?
    Contact the ADOA Service Desk through an email to AZNETSUPPORTDESK@ AZDOA.GOV or call 602-364-4444 Option 1.

13. What if I can't reset my PIN?
    Your new PIN cannot be the same as your old PIN. Try to use another 4-6 digit number combination. If that still does not work, contact the ADOA Service Desk through an email to AZNETSUPPORTDESK@ AZDOA.GOV or call 602-364-4444 Option 1.

14. What if Cisco AnyConnect is not on my computer?
    Please contact your agency IT department. They can assist you with installing the Cisco client on your system.

15. Who do I contact if I have questions about either VPN account?
    If you have a question about your existing VPN, contact the Service Desk through an email to **ServiceDesk@AZDOA.gov** or call 602-364-4444. If you have a question about your new VPN account, contact the AZNet Service Desk through an email to **AZNetSupportDesk@AZDOA.gov** or call 602-364-4444 Option 1.