DITO Technical Bulletin

Frequently Asked Questions about the New VPN

General

1. Why do we have to change from our current Citrix/AEP VPN system?

The previous implementation for remote access via VPN to IHS networks and data has reached the end of technical support by the vendor. Additionally, the capabilities and support requirements have changed over the years and require an updated system to support the needs of all IHS VPN users. This also includes the need to be technically compliant with new security requirements.

2. I was not notified to be migrated or provided with a two-factor authentication method. How do I get access to VPN?

Have your supervisor verify that you have approved VPN access via the online ITAC system. Your supervisor will then need to send a request to the IHS IT Service Desk to have your account migrated.

Please be sure to include in the request which form of two-factor authentication you will need. (You can also use your PIV card as a form of two-factor authentication by selecting "PIV" from the vRealm drop down.)

- If you will require the Entrust token, please provide a mailing address of the IHS Facility for us to ship the token to.
- If you will require the PhoneFactor, please provide the phone number that you will need to be called back on to verify your account.

3. Where can I find more information on how to use the IHS VPN?

Please see the IHS VPN User Guide.

4. What are the limitations to using RDS/RDP VPN?

See the appendix in the IHS VPN User Guide.

5. Who should I contact if I encounter a problem with the IHS VPN system?

If you have a problem, contact the IHS IT Service Desk:

Phone: 1.888.830.7280

E-mail: itsupport@ihs.gov

For after-hours support, contact the NOSC: nosc@ihs.gov

Authentication

6. Why do we have to use the Entrust token or Phone Factor authentication?

Two-factor authentication requires something you have and something you know in order to strengthen IHS security and user authentication. (You can also use your PIV card as a form of two-factor authentication by selecting "PIV" from the vRealm drop down.)

7. How do I switch to the token from PhoneFactor?

Discuss your needs with your supervisor to obtain approval. Your supervisor should then update your online ITAC form to change your two-factor authentication method. ITAC information can be found in the User Manual for the Information Technology Access Control (ITAC).

8. I lost my cell phone but need to use the VPN. How do I get access immediately?

Contact the IHS IT Service Desk (see Question #5 above), and we will assist you with a One Time Bypass set up on PhoneFactor.

Your supervisor should then need to submit a new request in ITAC to change your two-factor authentication method or update your PhoneFactor phone number.

9. I lost my Entrust token but need to use VPN. How do I get access immediately?

Contact the IHS IT Service Desk (see Question #5 above), and we will assist you with a temporary PIN code to access VPN.

Your supervisor should then need to submit a new request in ITAC for a replacement token.

10. I forgot my network password to get into VPN. What should I do?

Contact the IHS IT Service Desk to have them reset your D1 password.

11. I haven't used the IHS VPN system in several months and when I tried to use it, it just took me back to the login page. What should I do?

All VPN use is monitored and logged on a daily basis. Any VPN user who has not utilized the IHS VPN in over 60 days will be automatically deactivated per IHS policy. Requests for reactivation must be made by the employee's ITAC supervisor, who should first verify that the employee's ITAC indicates approval for VPN use, and then should send a request to the IHS IT Service Desk for reactivation.

12. When I try to log on at the IHS VPN logon site using PhoneFactor, it does not let me in or give me an error.

This may be due to a mismatch between the phone number defined for you in PhoneFactor and the one you are using for authentication. Please contact the IHS IT Service Desk to verify or change the phone number configured for you.

File Access

13. How do I find my network documents?

All of your files are located on the network share and network drives assigned to you as part of your network account and profile. (For assistance, contact your System Administrator.) These files can be accessed from the Start menu and select the Computer option to navigate to your files.

14. If I get disconnected from VPN, will I lose any documents that I was working on?

If using RDS/RDP, No. Your session and all applications will continue to run in the background for 24 hours for you to reconnect. You will not lose any unsaved documents unless you reconnect after the 24 hours. Best practice is to make sure that you save any documents to your network share. After 15 minutes of inactivity, your session will be disconnected but maintained for the 24-hour period and you will need to re-authenticate to get back into your session.

15. What are the timeouts when connecting to the IHS VPN?

The timeout when connected to the IHS VPN RDS/RDP desktop is set for 15 minutes of inactivity. However, if you get disconnected while you have any applications open, they will remain active for up to 24 hours with your session.

16. I need to transfer files from my computer to a remote server. What should I do?

You will need to request access to the SecureFTP program through the IHS IT Service Desk (see Question #5 above).

17. I can't see my entire screen when connected to the IHS RDS/RDP Desktop. What should I do?

You will need to use the Minimize option to change the size of the screen. Also, some RDS/RDP environments do not support the use of dual monitors when connected.

Applications

18. Can we have EHR installed?

Due to the large number of EHR site installations, this application, as well as other RPMS GUI applications, may not be supported within all RDS/RDP systems at this time. VPN users need to obtain the location of your facility or Area RDS/RDP or other location and use the Remote Desktop Protocol (RDP) to access that server/workstation for all RPMS GUI applications.

19. How do I get remote access to our facility EHR server (or any of the local RPMS GUI applications)?

Discuss your requirement with your facility/Area IT staff for the RDS/RDP or workstation where you have approval for access to EHR for your facility. (Use of Remote Desktop Services would be required.)

20. Why can't I install other applications that I need within RDS/RDP?

Restrictions for application installations are configured for Administrative rights for all workstations and servers. For any additional application that is required to perform your duties, please contact your local IT Service Desk (see Question #5 above) to request the application. If they cannot support the application within the RDS/RDP environment, you will be notified of an alternative option.

Connectivity Issues

21. I keep getting disconnected when using the IHS VPN (from home, the airport, a library, etc.).

This may be due to a poor network connection from the location you are using. Please try to connect from an alternate location or contact your local ISP to verify your Internet connectivity.

22. The hotel I am staying in is offering the use of a "Public IP address". What is it and do I need it?

You will need to use the DHCP IP address that will be provided by the hotel/public location. You will need to make sure that your laptop is not configured with a "static IP address." Please contact your local IT office for more information.

23. I have a Mac laptop. What do I need to do to be able to use IHS VPN?

Unfortunately, IHS does not support Mac computers.

Contact the IHS IT Service Desk (see Question #5 above) and they will be able to provide you with the Mac plugin and suggestions that may be required for you to access the IHS VPN.