DATAPIPE AUTH TWO-FACTOR AUTHENTICATION

ANYCONNECT INSTRUCTIONS

Thank you for choosing "Datapipe Auth", Datapipe's Two-Factor Authentication service. Please follow the instructions below to continue the setup of your Datapipe Auth solution using AnyConnect.

1. **Install the Java SE Runtime Environment on your workstation for AnyConnect** : Visit the below URL to download and install it for your workstation.
   http://www.oracle.com/technetwork/java/javase/downloads/jre8-downloads-2133155.html
2. **Ensure that your workstation/PC is synched with an accurate NTP resource:** The token is time-based. Make sure that it's synched otherwise a bad token will be generated. To do this, launch your Token Manager, log in to it (the same username and password for logging in to the Datapipe Auth Portal) and then click the left/right arrow button to switch to another token for your AnyConnect session (if you have more than one token).
3. **Visit the URL https://[your-primary-firewall-IP here]/**: From your workstation access your firewall IP. Click "Accept" when warned about the firewall SSL certificate. Enable/allow Java to run for your browser session (you will be prompted for action).
4. **Log in using your credentials**: Once you get the login windows, insert your username and PIN+token for the password field (the token generated by the token manager). **Please Note:** Make sure to use the correct token if you have more than one token.

After successful authentication, you will be prompted to install the Cisco AnyConnect Secure Mobility Client. Install it accordingly and your VPN session will be established after the installation.

If for any reason you find that you are disconnected/need to re-connect again, simply launch AnyConnect, key in your firewall IP and authenticate with your username and password (PIN+token).

Once you are connected, you should be able to RDP / SSH to your servers with the server's private IP.

Regards,

Datapipe Security Team