प्रणाली एवं आंकड़ा प्रबंधन महानिदेशालय,
केंद्रीय अप्रत्यक्ष कर एवं सीमा शुल्क बोर्ड
प्रथम तल टॉवर 1, एनबीसीसी प्लाजा,
सेक्टर 5, पुष्प विहार, नई दिल्ली-110017
adg.si@icegate.gov.in 011-29561543

## Advisory SI/01/2021 Dated: 08-01-2021

## RSA-2FA enablement for CBIC VPN w.e.f. 14/01/2021

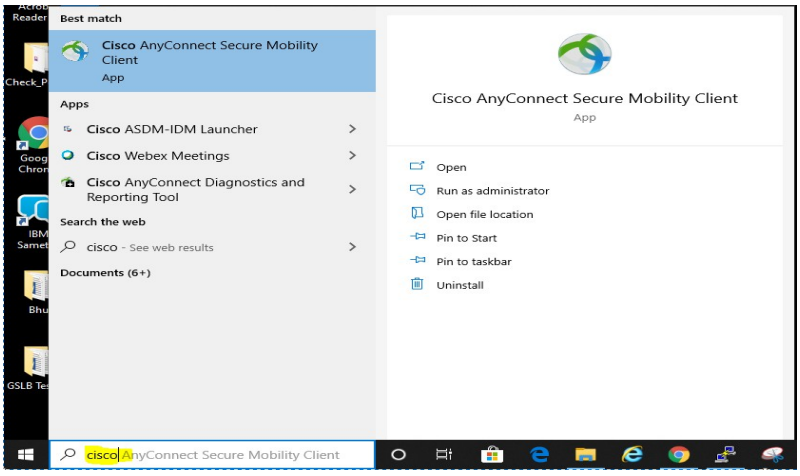
Many instances of misuse of user's VPN Id and password have come to the notice of DG Systems. Also at present, a VPN user has to remember separate passwords for VPN Id as well as that of SSO Id. In order to address these concerns, CBIC is launching RSA-2FA for VPN. With this enablement, a VPN user will not be issued VPN password and hence need not to enter VPN password while accessing VPN. In stead he/she has to enter RSA pin followed by OTP received on his/her registered mobile/e-mail Id (in case of on-demand authentication) or Passcode (in case of desktop-based authentication; Please Note that- passcode can be generated using RSA application which is available only for DG systems provided device). For details on RSA 2FA, please refer to Advisory SI/06/2019 on RSA SOP. RSA 2FA will lead to an additional layer of security to avoid unauthorized application access such as inappropriate usage of another user VPN Id and password.

2. Since DG Systems is enabling RSA-2FA for CBIC VPN users, having RSA pin becomes a mandatory perquisite for officers/ user using DG Systems VPN. So, if any VPN user are not having RSA pin, please follow steps referred at para 4.0 (Case I of Section I) and get it before **14/01/2021** to avoid any inconvenience.

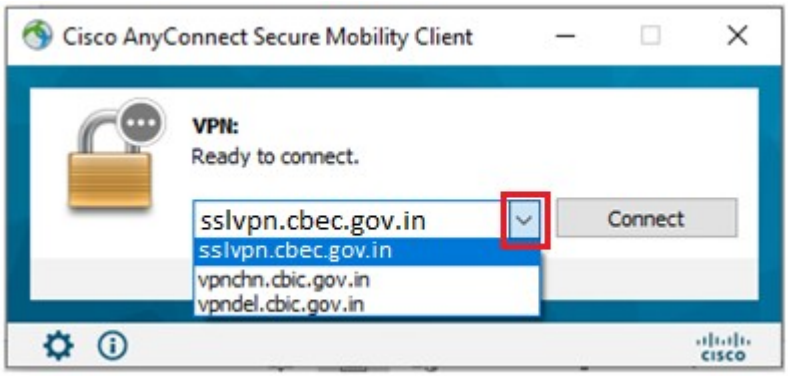
3. The process to connect RSA 2FA enabled VPN through AIO/Desktop/Laptop and ICETAB is elaborated under Section I and Section II respectively and will be effective from **14/01/2021**. The user must check and update his/her mobile no and e-mail id by accessing URL https://swayam.cbec.gov.in .

## Section I: RSA-2FA procedure for VPN users working on AIO/Desktop/Laptop

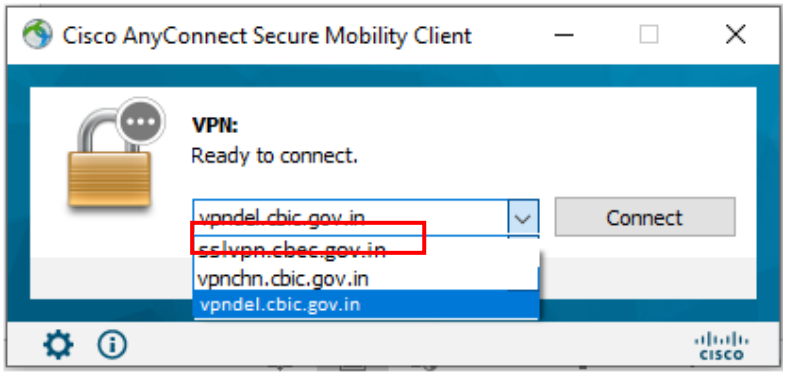
**1.** Search Cisco in Windows search bar and run Cisco AnyConnect Secure Mobility Client:



2. A window screen will pop up, click on the dropdown arrow. vpndel.cbic.gov.in and vpnchn.cbic.gov.in will appear in dropdown list as demonstrated below:




3. VPN user accessing Customs application or GST/Advait/ECCS application needs to select either Delhi DC URL vpndel.cbic.gov.in or Chennai DC URL vpnchn.cbic.gov.in and click on **Connect.**




****NOTE-** In case the users are unable to find the URLs i.e. vpndel.cbic.gov.in and vpnchn.cbic.gov.in in their respective dropdown list, they can type it manually in the above highlighted field.

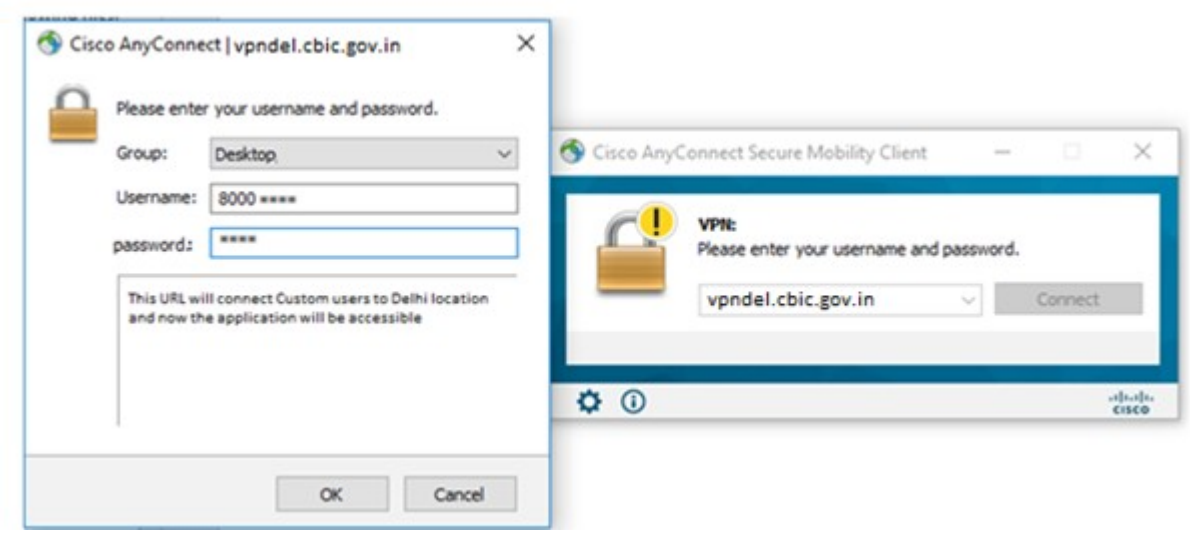
4. **Case I: Unregistered RSA Users-** The users whose RSA is not enabled

**4.1.1** Users need to update their contact details i.e. mobile number and email Id by following the steps mentioned in Case I and Case II of the SOP enclosed in the Advisory SI/08/2020.

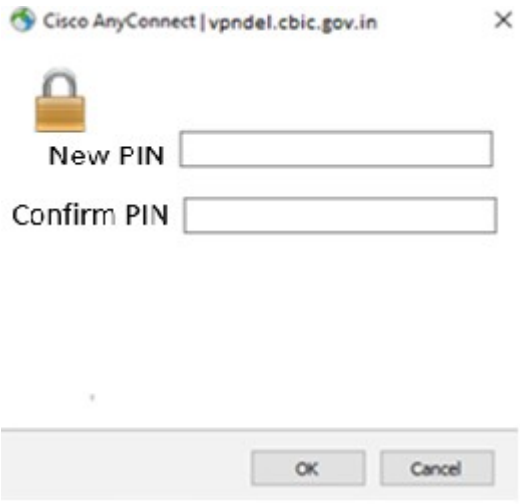
**4.1.2** After updating contact details, user needs to log Ticket with Saksham Seva at Saksham.Seva@icegate.gov.in requesting for RSA 2FA activation and issuance of RSA Pin.

**4.1.3** User will receive the default RSA pin from DG System Security team.

**4.2.1.** The user needs to enter the SSO ID under the **Username** and default PIN (received from Security team) under the **Password** and click on **OK**.

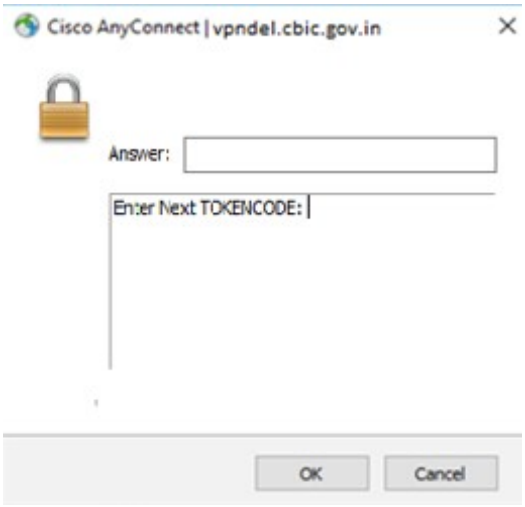



**4.2.2.** User will be asked to generate a new PIN (4-8 digits) and confirm the new PIN and click 'OK'

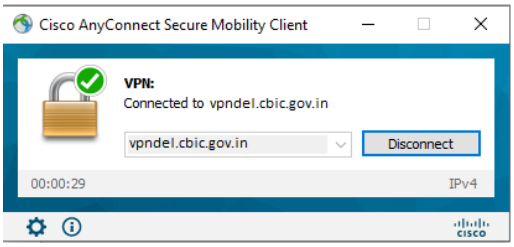



**Note**** This new pin will be used for subsequent logins.

**4.2.3.** Enter the OTP received on Mobile/e-mail Id (in case of on-demand authentication)/passcode (in case of desktop-based authentication) and click on '**OK**'.

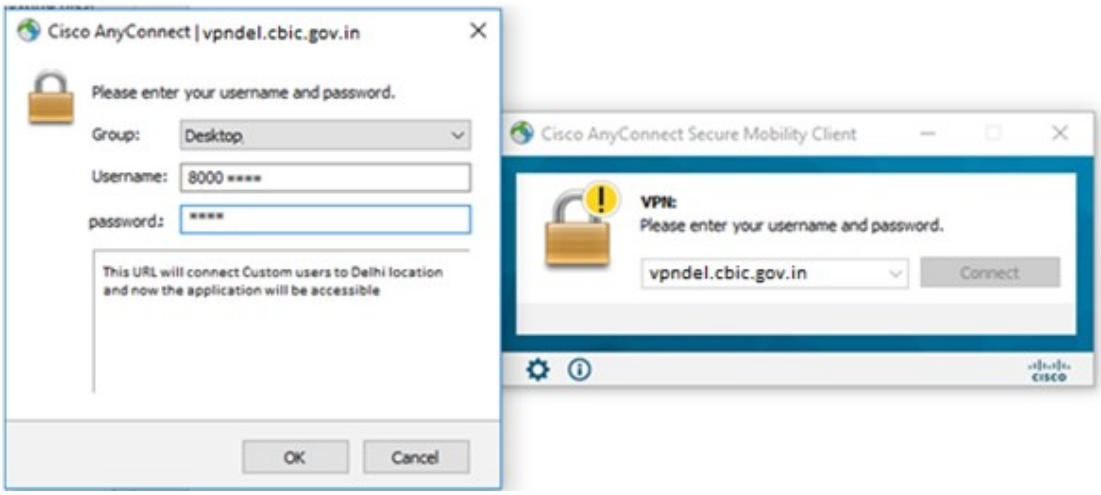



**4.2.4.** The user will be connected to VPN.

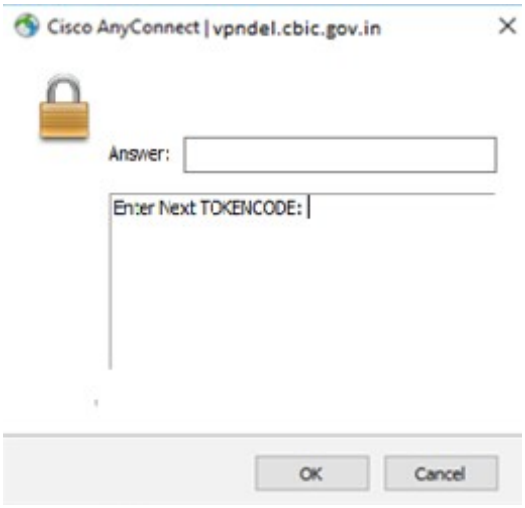



**5.0** **<u>Case II: RSA 2FA Enabled Users</u>**- The users who are already RSA 2FA enabled earlier

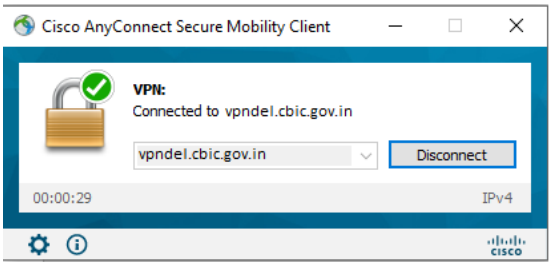
**5.1.** The user needs to enter the SSO ID under the **Username** and RSA PIN under the **Password** field and click on '**OK'.**




**5.2.** Enter the OTP received on Mobile/e-mail Id (in case of on-demand authentication)/passcode (in case of desktop-based authentication) and click on '**OK**'.



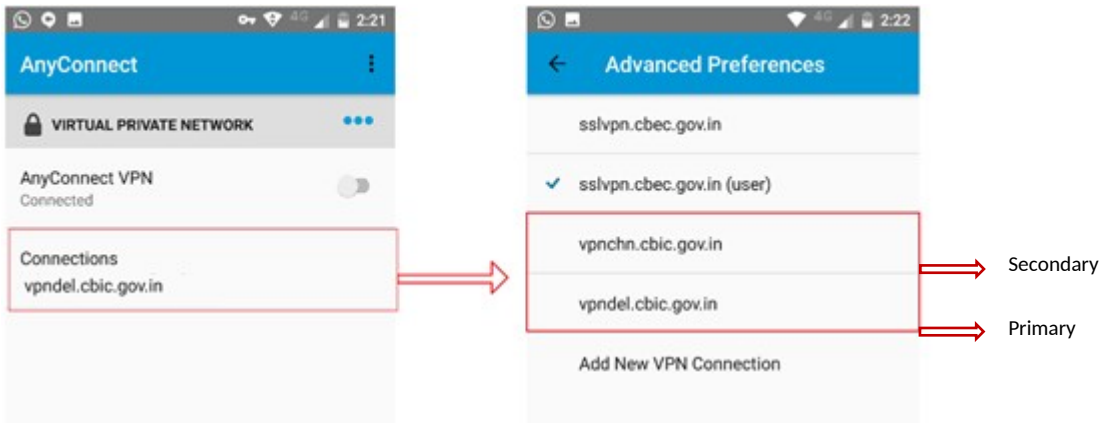

**5.3** The user will be connected to VPN.



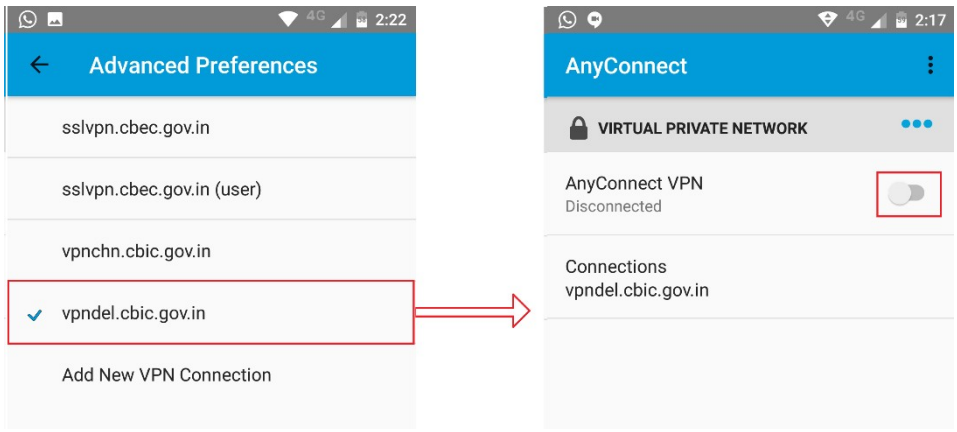

## Section II: RSA-2FA procedure for VPN users working on ICETAB

1. Search Cisco AnyConnect client application in ICETAB menu and launch it.

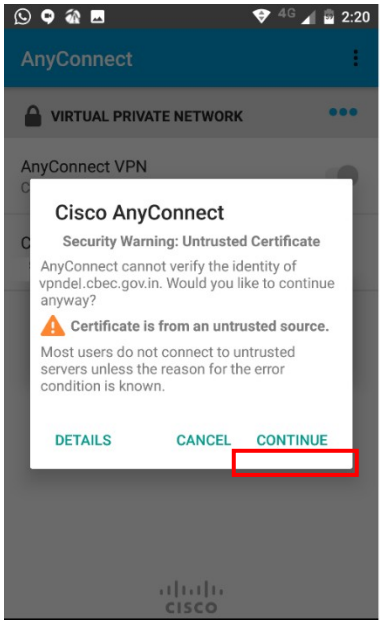

2. Click on **Connections** option where you will find both URLs, same as mentioned in below snap:



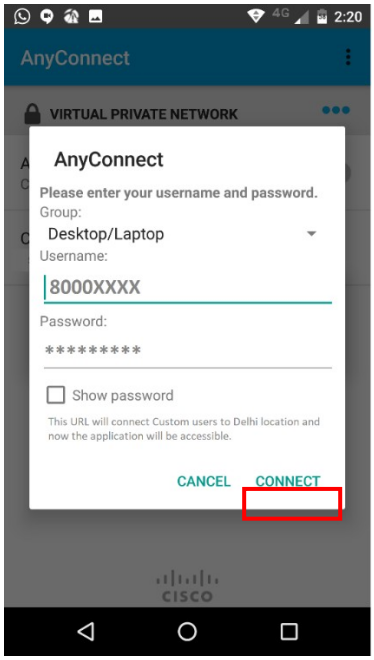

3. VPN user needs to connect VPN through either Delhi DC URL vpndel.cbic.gov.in or Chennai DC URL vpnchn.cbic.gov.in. Only this URL will be used in future for VPN connectivity.



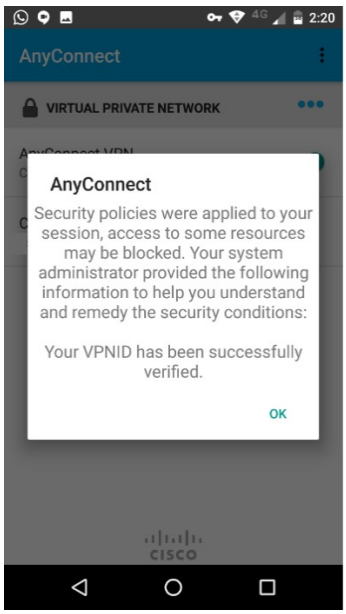

4. A window will be prompted for security warning, please click on 'Continue'.



5. The user needs to enter the SSO ID under the **Username** and RSA PIN under the **Password** and click on **'Connect'**.




6. Enter the OTP received on Mobile/e-mail Id (in case of on-demand authentication)/passcode (in case of desktop-based authentication).
7. Click on 'Connect'. The user will be connected to VPN.




**(Vinayak Chandra Gupta)**

Additional Director General (Systems)