VPN Remote Access FAQ

This document contains answers to some FAQs about the new RapidIdentity (formerly known as 2FA) MFA solution for VPN access.

1. **What is RapidIdentity?**
    a. RapidIdentity is a mobile app that is used for generating OTP codes similar to how existing RSA tokens function.
2. **What is an OTP?**
    a. OTP stands for One Time Password. This is the short numeric code that changes every 30 seconds and is used instead of a password for VPN access.
3. **Can I still use Cisco AnyConnect?**
    a. Yes, the same VPN client will be used and only the method of obtaining One Time Passwords will change to using a mobile app in most cases.
4. **Do I need to enroll in MaaS360 to use RapidIdentity?**
    a. Enrollment in MaaS360 is not necessary to use the RapidIdentity app. However, if you are a VPN user enrolled in MaaS360, the application can be automatically sent to your device.
5. **Can I use the RapidIdentity app on my personal device?**
    a. Yes, the application can be used on personal devices by downloading RapidIdentity from the iPhone or Android app stores. A phone number will need to be provided in order to receive the registration SMS text message.
6. **How do I register in the app once downloaded?**
    a. The easiest way is to send a SMS text message to a phone number associated with the user's account in the RapidIdentity administration console. The message contains a link to download the app and a second link to automatically enter the Server URL and username.
    b. For mobile devices that may not have a phone number (iPad etc), users can enter "**mfa.cityoftacoma.org**" in the Server URL field. When prompted, log in with your Windows username preceded with "tacoma\" and then select to use Windows password. Example: "tacoma\npeterson"
    c. For both of the above registration options, users should select to use their Windows password instead of an authorization code to enroll.
7. **What do I enter for credentials when prompted by AnyConnect?**
    a. Mobile app users only need to enter their OTP code in the password field. When using the RapidIdentity mobile app, you will be prompted to enter your PIN or fingerprint before the OTP code is generated.
    b. Hardware token users will also set a PIN number but will have to enter PIN+OTP in the password field. Example: If PIN=1234 and OTP=56789, password=123456789
8. **Can I still VPN if I do not have a smart phone?**

    a. Yes, there is still an option to use a traditional hardware token for individuals unable to use the mobile app.

9. **How do I enroll a hardware OTP token?**
    a. To enroll a hardware token, users will need to navigate in their web browser to **https://mfa.cityoftacoma.org/ONE** and log in with their Windows username and password. The system will prompt to enroll a new credential.
    b. Tokens can also be enrolled on behalf of the user by choosing "Log in as someone else" from the administration portal.

Other FAQ- Troubleshooting

Open your web browser and type http://ascot01/wra into the address line to access the Verdiem SURVEYOR Wake on Web home page

Internet Explorer issues

There may be issues with the pre-loading of software prior to login. This is usually caused by the site not being trusted. Please add the following URL's to the trusted sites in your Internet Explorer (see explanation below):

https://vpn.cityoftacoma.org

https://vpn1.cityoftacoma.org

https://vpn2.cityoftacoma.org

1. Open Internet Explorer.

2. Click on the "Tools" menu at the top of the window, then scroll down and click on "Internet Options".

3. In the window that appears, click on the "Security" tab.

4. Click on the "Trusted Sites" icon.

5. Click on the "Sites..." button. Another window will open.

6. Add the first URL listed above to the "Add this Web site to the zone:" slot (remember the 's' in https), then click the "Add" button.

7. Do the same for the other 2 URLs.

8. All 3 sites should appear in the “Web sites:” window when finished. Click the OK button twice and try to launch the VPN URL again.

If all of these fail you need to check your Internet Explorer security settings. If you have not already done so, add the above sites to the Trusted sites. If the install still fails, click the "Custom Level..." button after clicking the "Trusted Sites" icon on the "Security" tab of the Internet Options. Make sure either ActiveX, JavaVM, or Downloads are enabled.

ANTIVIRUS PROBLEMS

It’s critical that your home computer be running an antivirus program so that the risk is minimized that your home computer will infect any computers on the City’s network. However, Cisco, the company that provides our VPN connection hardware and software, is sometimes slow to keep up with the changing versions of different antivirus products. A particular antivirus product which has been allowing your home computer to connect in the past may suddenly fail the antivirus check and won’t let you connect. You could also encounter this problem the first time you setup the AnyConnect software and try to connect to the City’s network. If you get the message that your computer has failed the antivirus check, please consult your Department’s computer support representative(s) for the latest info on which antivirus software products are recommended and which are known to be a problem.

Recommended Antivirus software: MacAfee, AVG for free, Avira

If you have issues with running the AnyConnect installation here is a detailed look at what is happening.

The installer first tries to launch an ActiveX install. Many times you can catch the yellow bar across the top of the screen and allow the ActiveX session, but the installer may move past it quickly. Next the installer will try to push the AnyConnect software via Java. If this happens you should be challenged to accept some Java files (be sure to accept them). Finally the installer will attempt to download and run a file named similar to AnyConnect.exe (it will probably contain a version number somewhere in the file name). Accept the download and accept the security warning for running an un-trusted file.