Veracity Networks WCC: Remote Working Setup

Telework Overview

March 19, 2020

Contents

Remote Working

Best Practices for Telework

March 19, 2020

Remote Working – PC (Recommended)

- Your PC being used must be configured for use with WCC (see pages 7-11)
- Login to the online portal: https://portal.ccone.net
- If using Okta SSO, instead visit https://veracity.okta.com using your credentials.
  - If you do not have your credentials please contact your administrator.
- Enter in the DN being used to receive calls.
- This can be a cell phone, landline, or any other phone as long as the number can be dialed from the public network or private voice cloud
- Select the team to sign in as, and select “Save Changes”

Remote Working – Mobile

- Log in to the online portal: https://portal.ccone.net
- If using Okta SSO, contact your administrator as changes will need to be made by Veracity to allow logging in via mobile using your credentials
  - If you do not have your credentials please contact your administrator.
- Enter in the DN being used to receive calls.
- This can be a cell phone, landline, or any other phone as long as the number can be dialed from the public network or private voice cloud
- Select the team to sign in as, and select “Save Changes”

IMPORTANT NOTE: Using a Mobile device both to sign in to the Agent Desktop through a mobile browser and to take calls from WCC without using a WIFI connection but rather a mobile data connection from a carrier that does not support Dual Band will cause the agent desktop to forcibly log out as soon as a call is received.

System Requirements

System and Browser Requirements

March 19, 2020

Desktop System Requirements

- Memory: 2 GB RAM, excluding operating system allocation. Note that some applications may require more memory.
- Operating System: Supported operating systems are listed below. Other client operating systems can be used at the customer's discretion. Cisco will only provide best effort support and will not work on product fixes on unsupported operating systems
- Microsoft Windows: Windows 7, Windows 8 and Windows 10.
- Mac: OSX (when supported browsers are used)

Browser Requirements

- Supported Web browsers:
  - Internet Explorer 11.0 and above
  - Chrome version 40 and above
  - Firefox version 44 and above
- Required browser settings:
  - Browser cache cleared before starting the current release for the first time
  - Cookies: Enabled
  - Security level: Medium
  - Pop-up blocker: Disabled
  - JavaScript: Enabled
- Adobe Flash Player:
  - Adobe Flash Player 21 or later.
  - Download the latest version of flash from : https://get.adobe.com/flashplayer/
  - Identify the version of flash installed by launching : http://www.adobe.com/software/flash/about/

Agent Phones, Softphones, and DN -IMPORTANT

- Agent Phone, Softphones, and DN.
  - Agents require a phone with a direct dial number in order to use the Cisco agent application and have calls delivered to them.
  - Any type of phone may be used as long as the number can be dialed from the public network or private voice cloud.

- Voice Bandwidth
  - If a softphone is used, additional bandwidth of at least 100 Kbps per softphone instance is required.

Network Requirements/Recommendations

- All network appliances must be configured to allow unrestricted traffic between the client workstations and the following domains or IP subnets:
  - 208.77.192.0/24
  - 208.77.194.0/24
  - 208.92.127.0/24
  - 208.92.126.0/24
  - 208.50.136.0/26
  - *.transerainc.net
  - *.Ciscocc.net
  - *.Cisco.com
- Network appliances include the following devices:
  - Gateways
  - Routers
  - Hubs
  - Bridges
  - Switches
  - Proxy Servers
  - Firewalls
  - Load Balancers
- Firewalls must be configured to allow traffic on HTTP port 80 and HTTPS port 443 for the domains listed above.

Network Requirements/Recommendations

- **HTTP/Proxies**
  - Customers using HTTP/IP proxy devices, either directly or indirectly, must ensure that these devices are configured to exclude Cisco application traffic from any caching or authentication operations. The domain *.transerainc.net and *Ciscocc.net should be added to the proxy and firewall exclusion list.
- **Bandwidth and Latency**
  - High-speed Internet connection is required, with the minimum recommended speed being 512kbps.
  - The application request payloads can range from 1-100 KB each on the average, with peaks of 2 -3 MB.
  - Additional bandwidth of at least 100 kbps per softphone will need to be separately allocated for voice traffic
  - Round Trip Time: Network connectivity to the WCC data centers over the internet or private WAN must consistently provide less than a 250ms round trip time (RTT) and less than 1% packet-loss for acceptable performance