**SSO(Single Sign On) Enable One Token for Remote Login**

In efforts to reduce costs and enhance efficiency, you can enable Microsoft Authenticator to authenticate to all former CenturyLink systems and resources. This includes Cisco AnyConnect VPN, Global Protect VPN, CTL Jump Hosts, MyWorkSpace and Office 365 Applications. FLV3 systems are not included at this time. The previous CTL authentication system – Known Access (NACID, SecurID, SMS and NACPASS) has been decommissioned.

1. You’ll need a working Microsoft Authenticator token.

To use **Microsoft Authenticator,**ensure that you already have Microsoft Authenticator set up on your mobile phone. If not, go to <https://mfa.centurylink.com> for Microsoft Authenticator set up instructions within the selectable tab. After setting up Authenticator proceed to step 2 and select the link.

1. 

Go to <https://mysupportdesk.service-now.com/msd?id=msd_index>

1. 

Search for “Single Token”

1. 

Select the “Single Token Use Request” Form

1. 

Fill out the “Requested For Section” with your name. Select your preferred token type and WAIT for token Check to display a message

1. 

If Token Check box displays “Requester has token” click submit and you’ll be added to the correct single token group.

If Token Check box displays “Requester does NOT have token” you will be redirected to get a token. After your request has been submitted, it can take up to 40 minutes to sync from ServiceNow to our downstream processes.

ServiceNow also may take overnight to recognize your new token setup, so if that happens or if any issues are encountered, open up a ticket with the Help Desk via chat or phone call at 877-828-4357 for immediate assistance.