

Multi-Factor Authentication for device login using ISE and OKTA

PRE-REQUISITE-

Users should have OKTA app in mobile and registered with Genpact OKTA services.
Users should have account in AD and ISE.

SOP FOR LOGIN TO DEVICES-

1. We'll use the Okta Verify application already installed and used to access GSocial and MyTime services.
2. SSH into any Network Device.
3. Enter OHR ID and associated AD credentials
4. Select any of the below options-
 - a. To input unique key
 - b. To initiate a push on mobile



```
703271545@GCPLINHYD2MW01:-  
| Anyone using this system expressly consents to such monitoring |  
| and is advised that if such monitoring reveals possible |  
| evidence of criminal activity, system personnel may provide the |  
| evidence of such monitoring to law enforcement officials. |  
+-----+  
Password:  
Please select your second authentication method [num]:  
1 - Okta Verify.  
2 - Okta Verify Push.  
Enter '0' to abort.  
  
C  
C  
"You are accessing a restricted device"  
C  
CC  
+-----+  
| The level now being accessed and information available through |  
| this equipment is highly confidential and proprietary. It may be |  
| accessed or used only as specifically authorized. All other access |  
| or use is prohibited and is subject to legal action! |  
+-----+  
IND-WOI-GSD-COR-SW-01#
```

5. Login into the device will be successful after completion of the above Multi-Factor Authentication.