**Purpose:**

To install Crowdstrike (falcon-sensor) on RHEL8 (or similar) on the UBC VM system.

|  |  |  |
| --- | --- | --- |
| **Step** | **Major Activity** | **References, Forms and Details** |
| **1** | Obtain the RPM and the CID from UBC IT   * falcon-sensor-5.38.0-10402.el8.x86\_64.rpm * CID | * CID = customer ID, obtained from UBC IT |
| **2** | Install the package   * dnf install falcon-sensor-5.38.0-10402.el8.x86\_64.rpm | * Will install at /*opt/*Crowdstrike |
| **3** | Install the CID   * */opt/*Crowdstrike/falconctl -s –cid={provided cid} | * Double-dash ahead of “cid=” |
| **4** | Enable Crowdstrike daemon   * systemctl enable falcon-sensor | * Will start upon startup |
| **5** | Start Crowdstrike   * systemctl start falcon-sensor |  |
| **6** | Check everything working   * systemctl status falcon-sensor | Should see:  falcon-sensor.service - CrowdStrike Falcon Sensor  Loaded: loaded (/usr/lib/systemd/system/falcon-sensor.service; enabled; vendor preset: disabled)  Active: active (running) since Wed 2021-07-14 14:53:31 PDT; 3min 32s ago  Process: 255872 ExecStart=/opt/CrowdStrike/falcond (code=exited, status=0/SUCCESS)  Process: 255871 ExecStartPre=/opt/CrowdStrike/falconctl -g --cid (code=exited, status=0/SUCCESS)  And  . . .  CrowdStrike(4): Connected directly to ts01-b.cloudsink.net:443  CrowdStrike(4): ValidateCertificate: Certificate verified!  CrowdStrike(4): SSLSocket connected successfully to ts01-b.cloudsink.net:443  CrowdStrike(4): sock/ssl/proxy cnctd ok. First send to cloud.  CrowdStrike(4): CLOUDPROTO\_ESTABLISHED. AgentId unchanged  CrowdStrike(4): ConnectToCloud successful. |
| **7** | Check the log   * cat *var/*log/falcon-sensor.log | * May be blank |