- First download the FortiSIEM agent (`FSMLogAgent.exe`)
- we need to execute some prerequisites before doing the installations
  - Agent must upload event data to a collector >> minimum architecture is (one Super appliance + one Collector appliance)
    - that's why we did the installation of collectors in previous section
  - Without TLS 1.2 enabled, Windows agent installation will fail. use below command to add the registry key (run this in CMD as admin)

```
REG ADD
"HKLM\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Prot
ocols\TLS 1.2\Client" /v DisableByDefault /t REG_DWORD /d 00000000
```

  - Switch off Disk Fair share (this is the feature in windows, this actually conflict with the UBA (User Behavioral Analytics) Agent) - if you want to read about this feature check microsoft documentation - type this in powershell

```
$temp = (gwmi win32_terminalservicesetting -N
"root\cimv2\terminalservices")

$temp.enableDiskFSS = 0

$temp.put()
```

```
- now you can run the FortiSIEM agent

*Note:*
- Agent host name should exactly match your computer name (you can check
in system information) (in CLI method, this is not required)
- organization name is `Super` and organization ID is `1` by default for
`Enterprise` edition
- for `Agent Username` and `Agent Password`, first we need to create
this account in FortiSIEM before doing the installation
        - To create this go to `FortiSIEM > CMDB > Users > Ungrouped >
New`, don't forget to check `System Admin` then `Agent Admin` > back and
save
```

- Run this command
```bash
        FSMLogAgent.exe SUPERNAME="<ip>" SUPERPORT="<port>"
ORGNAME="super" ORGID="1" AGENTUSER="<agentuser>" AGENTPASSWORD="
<agentpassword>" HOSTNAME="" SSLCERT="0" /quite
```

- to double-check if things are working fine and to check if the agent is installed, open `Services` and search for `FSMLogAgent` and check the status (it should be `running`)
- now return to `FortiSIEM` and go to `ADMIN > Health > Agent Health` - you will get the full details.
    - now you can see that `Agent Status` as `Registered` and not yet running, we need to do one more action
    - go to `CMDB` , if you get Status as unmanaged, just highlight it and check `Actions > Change Status > Approved`
    - to make the status as running active is to associate this window to collector.
        - to do this return back to `ADMIN > Setup > Window Agent`, and here you will see the configuration for the `windows agent monitoring and associating`. monitoring template is nothing but to select the module that you need to activate like UBA or whatever logs you want to monitor
        - select `New > Generic` , give name
        - in the `New > Event > New` , `Type` as security, windows powershell, etc. also you can select `IIS` and `DHCP` if you have the server running the services
    - in `UEBA` , just check the checkbox
    - you can also check for any registry change for the key registry values, you can check the "installed software change" and "removable drive"
    - in `Script` section, you can add some `WMI Classes` and `Powershell Script` to collect extra information and then save
    - the association done in `Host To Template Associations` path, create `New` and give name and select the host and add it to the selection and select the template created previously and select the collector and save
- now go to the `CMDB` and check the `Agent status` it should be `Running Active` now, which means that the agent now able to communicate with the collector.

- to check if its logging, go to `Analytics` tab and look for this windows ip and try to run some powershell commands in the windows and then come back here and check the logs