

## Immediate Insight – Free Community Edition - Quick Start Guide

**Important Note:** *sizing pre-requisites & install instructions below assume the free community edition of Immediate Insight which allows concurrent search of 25 million events. A paid production scale implementation of Immediate Insight supports billions of event, but requires a different installation environment with more computing resources. For detailed install instructions for a full production scale deployment, please contact [ijsupport@firemon.com](mailto:ijsupport@firemon.com)*

### Installing on VMWare Workstation / VMWare Player (version 8 or newer)

These are the basic steps to install the free community edition of Immediate Insight using VMWorkstation (also works on Fusion). First download Immediate Insight OVA file provided by FireMon to your computer. (about 1 GB). Internet connectivity is assumed in these instructions.

1. from VMWare Workstation Import the OVF
  - File > Open (a Virtual Machine)
  - Open, then Import the OVA file you just downloaded
2. Edit the Virtual Machine Settings before starting the VM
  - Add a 2<sup>nd</sup> virtual hard drive for data storage, 40 GB is recommended (the 1<sup>st</sup> drive uses 20 GB)
    - Create a New Virtual Disk
    - Store Virtual Disk as a single file, and configure the disk size
    - Optionally, but suggested, you may select 'Allocate all the disk space now'
  - Set the RAM & CPUs
    - the recommended size is 4 total Processor cores, & 8 GB of Memory
  - Network Adapter
    - Specify "Bridged"
  - Start the VM
3. Login from the VMWare Console to configure IP Address and other settings by:
  - Connect to the VM via the Console in VMWare Workstation
  - Login to the Immediate Insight CLI as user:insight password:WhatsHappeningNow
  - type 'install' and follow the prompts to configure the system
  - Asks you to install server, or agent (choose server unless instructed by FireMon Support)
  - Specify the IP address (specify static values, or if dynamic type 'dhcp' at the IP Address prompt)
  - When prompted for NTP servers, accept the defaults or change to another valid NTP server.
  - if you are using an SSD drive, specify Y when prompted
  - When asked if you want to join a Cluster specify N
  - Type 'date' to verify timezone is correct.
  - if not, 'set-timezone' to fix it
  - type "sudo reboot" (note: the password for superuser/sudo is also WhatsHappeningNow)
  - after reboot login to the CLI, then type 'start' to launch the software
3. Login from a browser (Chrome is the supported browser)
  - If you don't already know the IP Address, you can get it by typing 'status' at the CLI
  - From Chrome go to the URL <http://youripaddress:3201>
    - Note: if you want to use HTTPS, you must first type 'set-ssl on' at the CLI
  - Login as user:admin password:admin (*the free community version does not require a license*)
4. Add some initial data to search
  - The easiest way to do this to go the Data Flow > Import screen
    - Drag & Drop a few LOG &/or PCAP files into the 'Import as Lines' (use Import Time 'Now')
  - Then go to Search tab, and click the 'Search' button to the right of the search string
    - navigate to different views of the data (e.g. Events, Entities, Most Common)

Training Videos are available at <https://www.firemon.com/resources/media/immediate-insight/>  
 For more detailed documentation or assistance please contact [ijsupport@firemon.com](mailto:ijsupport@firemon.com)