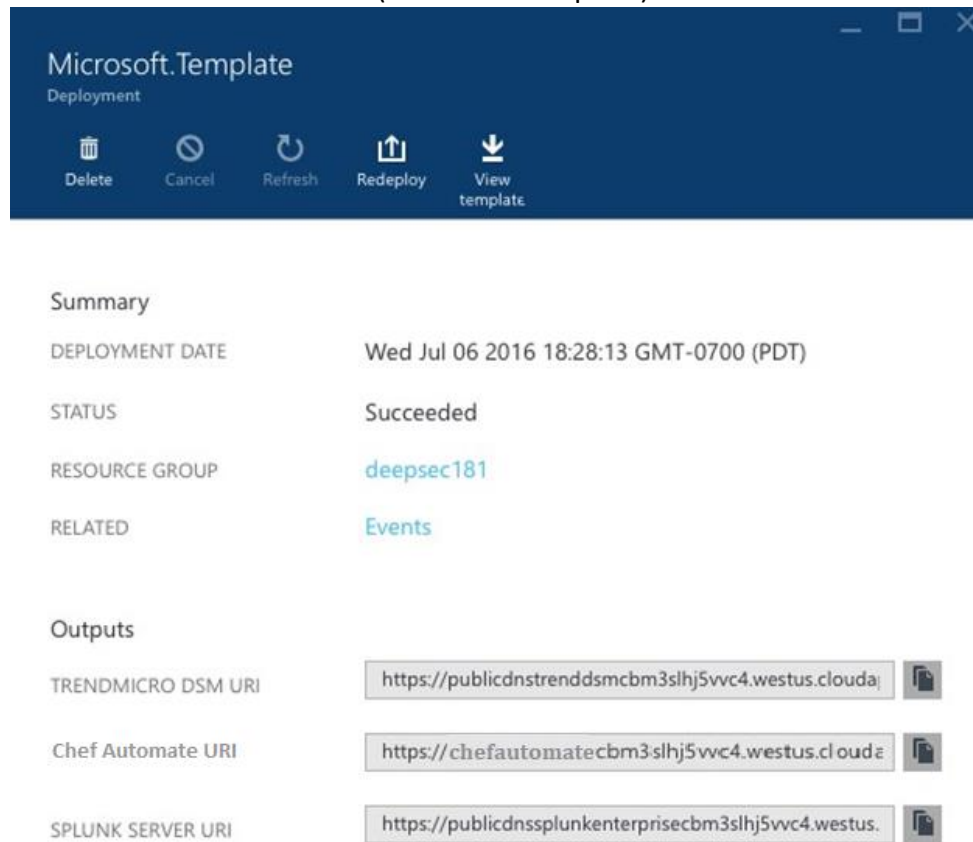From the output section of the deployment you can get the URL for TrendMicroDSM, Splunk and Chef Automate Server (Microsoft.Template)

To login to TrendMicro DSM
- Paste the TrendMicro DSM URL in the browser
- Enter the **Username** and **Password** provided in the parameter section during the deployment
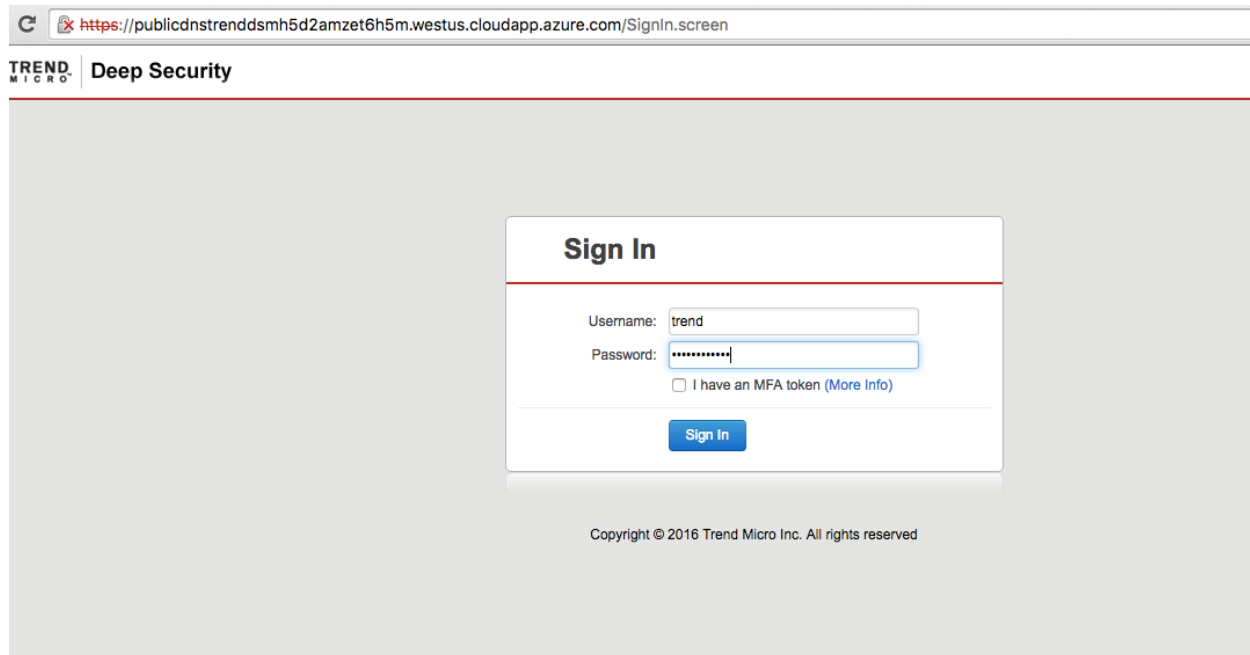
In order to send the system logs Splunk
- Go to **Administration** on the menu bar and select "SIEM" under "System Settings"
- Check "Forward System Events to a remote computer"
- In the "Hostname or IP address" text box enter Splunk FQDN
- In UDP port textbox enter port **5005** (default port is 514)
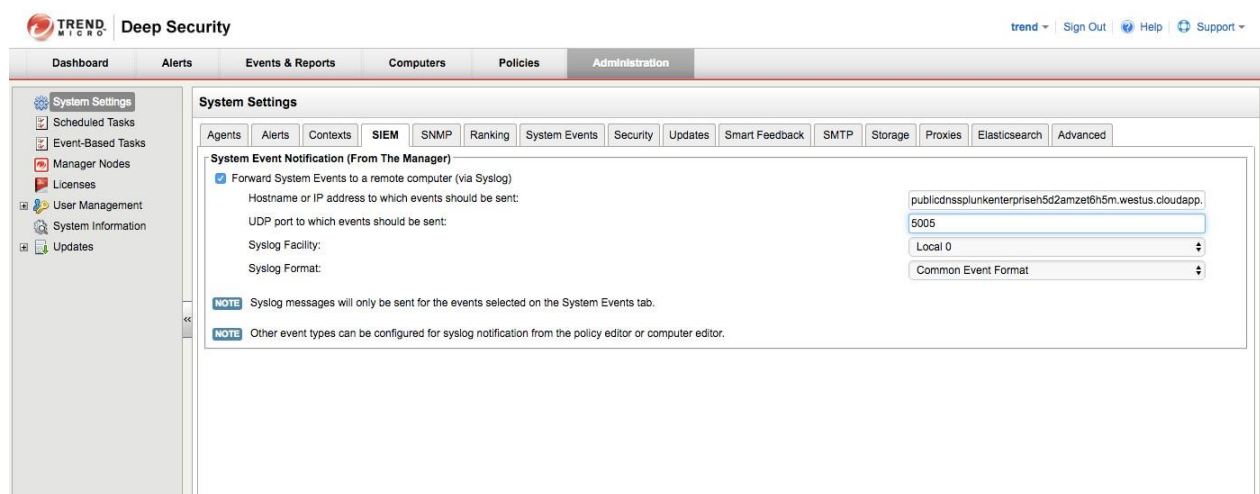
In order to forward the Security events to Splunk

- Select "Policies" in the menu bar
- Click on the "Base Policy" which opens a pop-up
- In pop-up screen go to settings and select "SIEM"

- In all the sections, select "Forward Events To" and "Relay Via Manager"
- In the "Hostname" textbox enter Splunk FQDN and in "Port" textbox enter "5005"
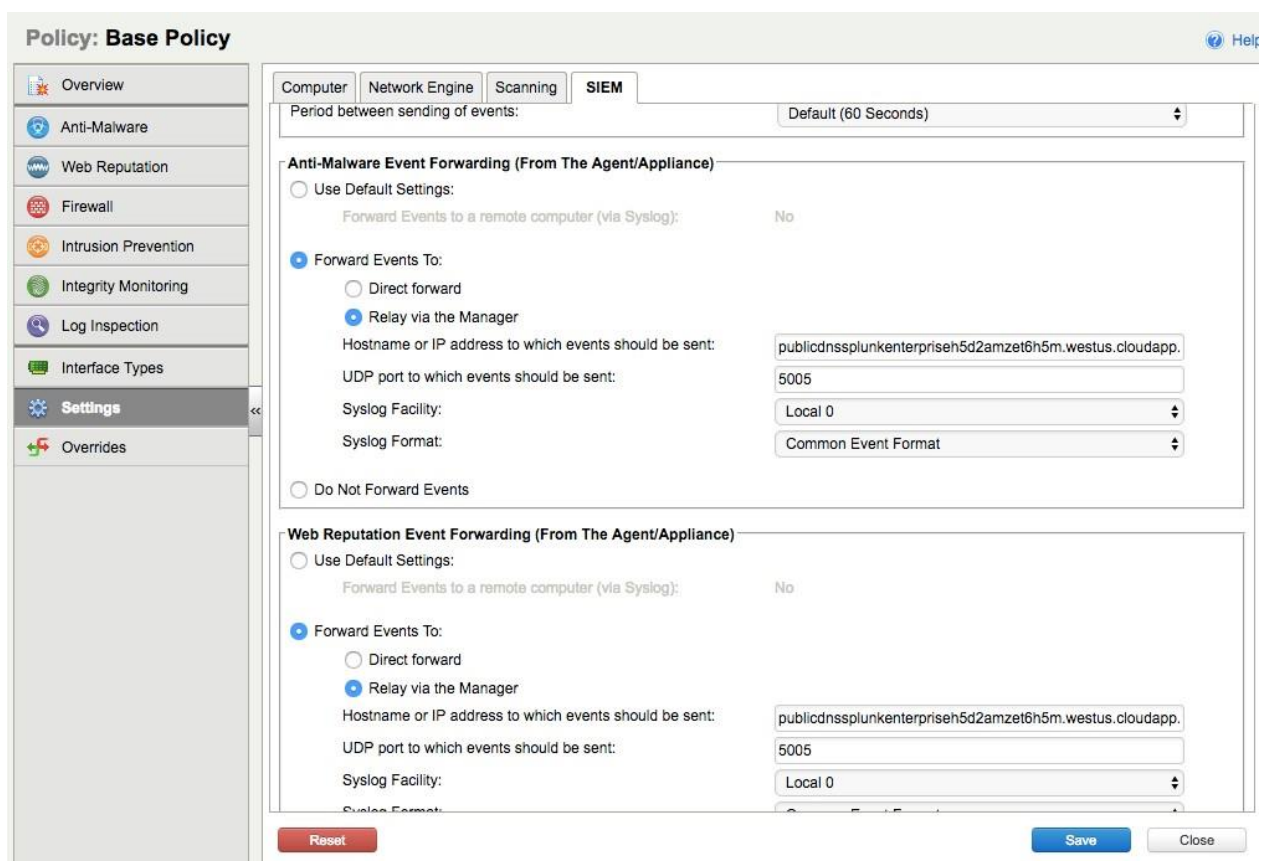
Apply policies to agents that are managed by Deep Security Manager

In the previous step we configured to send all the Security events to splunk, now all the computers (agents) that has been assigned with any policy under Base Policy will inherit the same SIEM settings

- Go to "Computers" from the main menu

- Click on any computer to open a pop-up, where you can see all the settings that can be done
- Under "Overview"à"General" select Policy in the "Policy" dropdown (linux policy for linux machine) and (windows 2012 policy for windows)
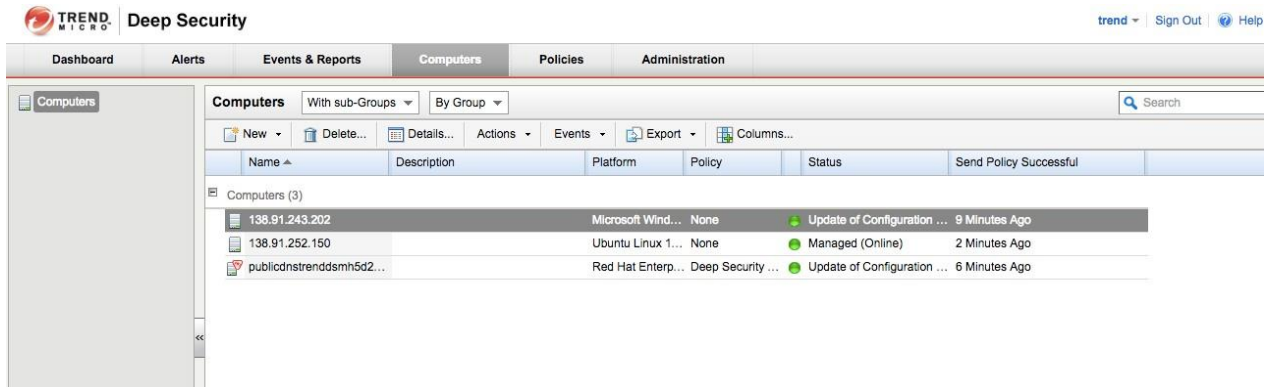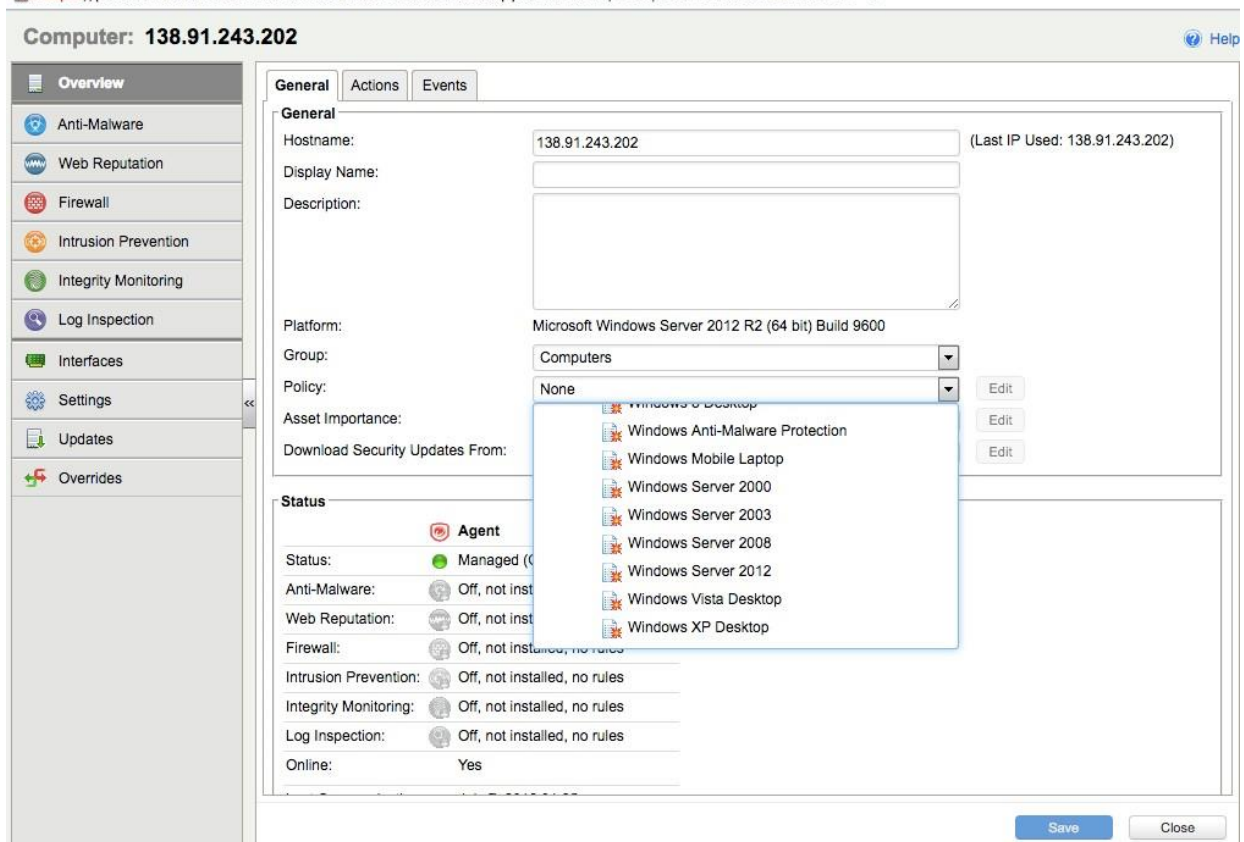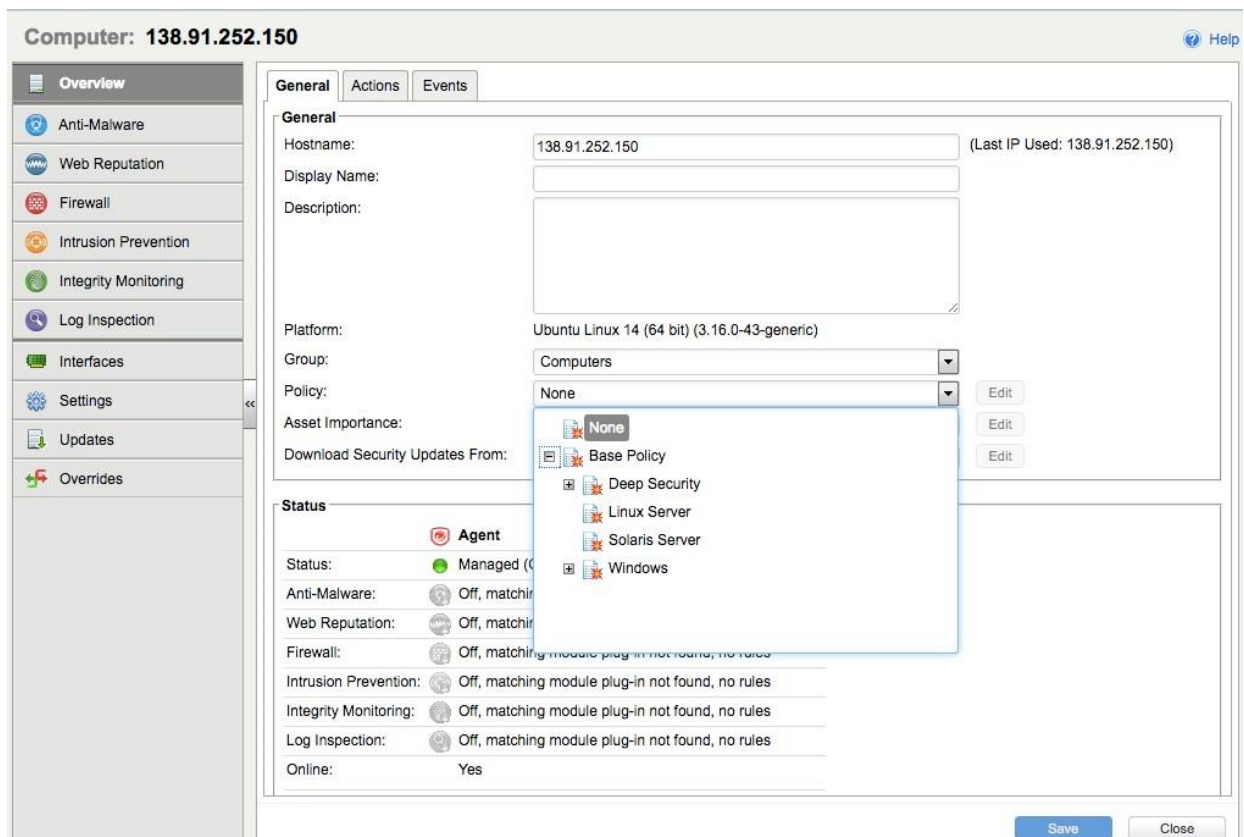
All the configurations are done on the TrendMicro DSM, so now all the system and security logs will be sent to Splunk.

Login to Splunk

Using the Splunk URL, open the Splunk Enterprise webpage
Enter Username – **admin** and password that is entered in paramaters section during deployment.
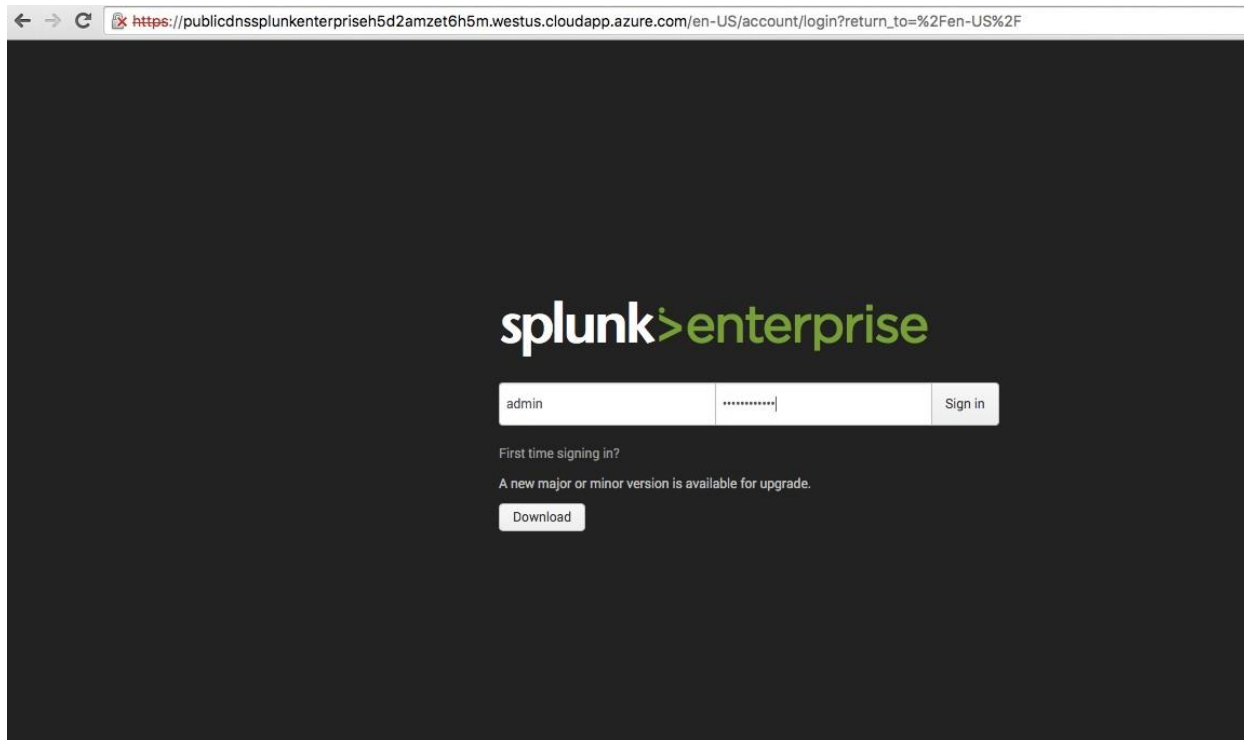
After login, you will see the below screen where "Trend Micro Deep Security for Splunk" (red color) app is already installed
Also in the Settings->input data, port 5005 is setup
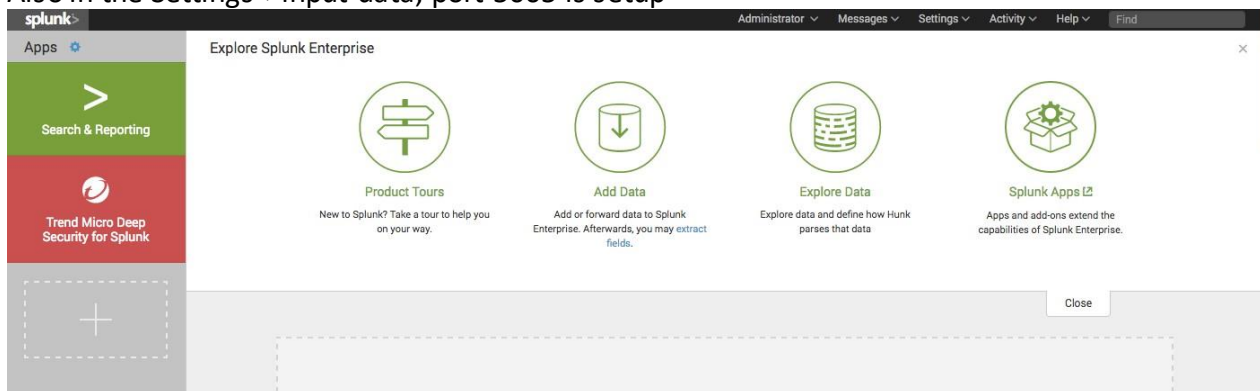
Click on the "Trend Micro Deep Security for Splunk" where you can see the below screen which shows the logs are being collected by splunk

splunk>   App: Trend Micro Deep Security for Splunk ⌄   Administrator ⌄   Messages ⌄   Settings ⌄   Activity ⌄   Help ⌄   Find

Search   Dashboards ⌄   Saved Searches ⌄   TREND Deep Security

🔍 New Search   Save As ⌄   Close

host="40.118.170.82"   All time ⌄   🔍

✓ 22 events (before 7/7/16 12:31:03.000 AM)   No Event Sampling ⌄   Job ⌄   ‖   ■   ↗   🖨   ⬇   💡 Smart Mode ⌄

Events (22)   Patterns   Statistics   Visualization

Format Timeline ⌄   — Zoom Out   + Zoom to Selection   ✕ Deselect   1 minute per column

List ⌄   ✏ Format ⌄   20 Per Page ⌄   ‹ Prev   1   2   Next ›

‹ Hide Fields	☰ All Fields	ⅼ	Time	Event
Selected Fields ɑ host 1 ɑ source 1 ɑ sourcetype 2		>	7/7/16 12:29:24.000 AM	Jul 7 00:29:24 40.118.170.82 Jul 7 00:29:20 trendMicroDSM CEF:0|Trend Micro|Deep Security Manager|9.6.21939|151|Software Added|3|src=10.7.0.4 suser=System target=Agent-Windows-9.5.3-5500.i386.zip msg=Description Omitted TrendMicroDsTenant=Primary TrendMicroDsTenantId=0 host = 40.118.170.82 source = udp:5005 sourcetype = deepsecurity-firewall communicate network
Interesting Fields ɑ act 1 ɑ action 1 # bytes_in 4 ɑ cef_product 2 ɑ cef_prodversion 1 # cef_ruleid 8 ɑ cef_rulename 8 # cef_severity 2 ɑ cef_vendor 1 # cef_version 1		>	7/7/16 12:29:08.000 AM	Jul 7 00:29:08 40.118.170.82 Jul 7 00:25:50 trendMicroDSM CEF:0|Trend Micro|Deep Security Agent|9.6.21939|153|Invalid TCP Timestamp|5|cn1=1 cn1Label=Host ID dvchost=publicdnstrenddsmh5d2amzet6h5m.westus.cloudapp.azure.com TrendMicroDsTenant=Primary TrendMicroDsTenantId=0 act=Log dmac=00:0D:3A:33:EA:F5 smac=12:34:56:78:9A:BC TrendMicroDsFrameType=IP src=24.18.144.209 dst=10.7.0.4 in=0 cs3= cs3Label=Fragment ation Bits proto=TCP spt=55317 dpt=443 cs2=ACK cs2Label=TCP Flags cnt=4 host = 40.118.170.82 source = udp:5005 sourcetype = deepsecurity-firewall communicate network
		>	7/7/16 12:29:08.000 AM	Jul 7 00:29:08 40.118.170.82 Jul 7 00:25:50 trendMicroDSM CEF:0|Trend Micro|Deep Security Agent|9.6.21939|153|Invalid TCP Timestamp|5|cn1=1 cn1Label=Host ID dvchost=publicdnstrenddsmh5d2amzet6h5m.westus.cloudapp.azure.com TrendMicroDsTenant=Primary TrendMicroDsTenantId=0 act=Log dmac=00:0D:3A:33:EA:F5 smac=12:34:56:78:9A:BC TrendMicroDsFrameType=IP src=24.18.144.209 dst=10.7.0.4 in=54 cs3= cs3Label=Fragmen tation Bits proto=TCP spt=55301 dpt=443 cs2=ACK cs2Label=TCP Flags cnt=1 host = 40.118.170.82 source = udp:5005 sourcetype = deepsecurity-firewall communicate network
		>	7/7/16 12:29:08.000 AM	Jul 7 00:29:08 40.118.170.82 Jul 7 00:23:20 trendMicroDSM CEF:0|Trend Micro|Deep Security Agent|9.6.21939|153|Invalid TCP Timestamp|5|cn1=1 cn1Label=Host ID dvchost=publicdnstrenddsmh5d2amzet6h5m.westus.cloudapp.azure.com TrendMicroDsTenant=Primary TrendMicroDsTenantId=0 act=Log dmac=00:0D:3A:33:EA:F5 smac=12:34:56:78:9A:BC TrendMicroDsFrameType=IP src=24.18.144.209 dst=10.7.0.4 in=0 cs3=DF 0 cs3Label=Fra gmentation Bits proto=TCP spt=55308 dpt=443 cs2=ACK PSH FIN cs2Label=TCP Flags cnt=1