Deep Discovery Inspector is a third-generation threat management solution that delivers advanced persistent threat (APT) and targeted attack visibility, insight, and control. Deep Discovery Inspector provides IT administrators with critical security information, advanced persistent threat (APT) and targeted attack visibility, insight, and control. Trend Micro recommends using a custom network for sample analysis. Custom networks ideally are connected to the Internet but may be configured with their own network settings. The appliance provides the option to configure proxies for custom networks, as well as providing support for proxy authentication. The networks must be independent of each other so that malicious samples in the custom network do not affect hosts in the management network.

To plan your network deployment environment, see the Deployment section in the Installation and Deployment Guide.

**Deployment Checklist**

<table>
<thead>
<tr>
<th>Requirement</th>
<th>Details</th>
</tr>
</thead>
<tbody>
<tr>
<td>Activation Code</td>
<td>Obtain from Trend Micro</td>
</tr>
<tr>
<td>Monitor and VGA cable</td>
<td>Connects to the VGA port of the appliance</td>
</tr>
<tr>
<td>USB keyboard</td>
<td>Connects to the USB port of the appliance</td>
</tr>
<tr>
<td>Ethernet cables</td>
<td>One cable connects the management port of the appliance to the management network, and one connects the appliance to a switch or router. The appliance is the default is 255.255.255.0</td>
</tr>
<tr>
<td>Internet-enabled computer</td>
<td>A computer with the following software installed: Google Chrome, Microsoft Internet Explorer 11.0, Microsoft Edge, Mozilla Firefox</td>
</tr>
<tr>
<td>IP addresses</td>
<td>One static IP address in the management network, and one additional IP address for an internal Virtual Analyzer, if connected to a custom network with Internet connectivity</td>
</tr>
</tbody>
</table>

**Setting Up the Hardware**

1. Mount the Deep Discovery Inspector appliance in a standard 19-inch 4-post rack, on a free-standing object, such as a sturdy desk.
2. Connect the appliance to a power source.
3. Connect the monitor to the VGA port at the back of the appliance.
4. Connect the keyboard and mouse to the USB ports at the back of the appliance.
5. Connect the management port to your network.
6. Power on the appliance.

**Performing Initial Configuration: Preconfiguration Console**

Perform the initial preconfiguration from the Preconfiguration Console with any of the following:
- VSA port
- Serial port

For details on how to access the Preconfiguration Console, see the Preconfiguration chapter in the Installation and Deployment Guide.

1. On the Preconfiguration Console login screen, type the following default login credentials:
   - User name: admin
   - Password: admin

2. On the Preconfiguration Console main menu, type 2 to select Device Settings and press Enter.
   - To set a static IP address: Use the space bar to toggle the IP address option to dynamic.
   - To set a static IP address:
     A. In the Type field, use the space bar to toggle the IP address option to static.
     B. Type the following network settings:
        - IP address (IPv4): the default is 192.168.252.1
        - Subnet mask: the default is 255.255.255.0
        - (Optional) Gateway: the default is 192.168.252.254
        - (Optional) DNS Server 1
        - (Optional) DNS Server 2
   4. (Optional) Type a VLAN ID.
   5. Navigate to Return to main menu and press Enter.

The initial configuration is complete and the management console is accessible.

**Performing Initial Configuration: Management Console**

1. Using a supported web browser, open the management console at
   - http://<Deep Discovery Inspector IP Address>:

   **Note:** Deep Discovery Inspector 3.8 and above can be deployed in IPv6 environments.

2. On the logon screen, type the following default credentials:
   - User name: admin
   - Password: admin
3. Click Log On.
4. Type a new password, and then retype it to confirm.
5. On Administration > System Settings > Time, set the system time.
7. To configure post-deployment settings, follow the steps in the Setup Guide. For details on how to set up your threat protection, see the Get Started chapter in the Administrator’s Guide.
8. Populate additional IP addresses for internal Virtual Analyzer, if connected to a custom network with Internet connectivity.
9. For details on how to access the Preconfiguration Console, see the Preconfiguration chapter in the Installation and Deployment Guide.
10. On the Preconfiguration Console login screen, type the following default login credentials:
    - User name: admin
    - Password: admin

11. On the Preconfiguration Console main menu, type 2 to select Device Settings and press Enter.
    - To set a static IP address: Use the space bar to toggle the IP address option to dynamic.
    - To set a static IP address:
      A. In the Type field, use the space bar to toggle the IP address option to static.
      B. Type the following network settings:
         - IP address (IPv4): the default is 192.168.252.1
         - Subnet mask: the default is 255.255.255.0
         - (Optional) Gateway: the default is 192.168.252.254
         - (Optional) DNS Server 1
         - (Optional) DNS Server 2
13. (Optional) Type a VLAN ID.

The initial configuration is complete and the management console is accessible.

**Recommended Network Environment**

Deep Discovery Inspector is deployed offline. This means that Deep Discovery Inspector does not interrupt network traffic. A switch monitors both internal and external traffic and passes the information to Deep Discovery Inspector. Deep Discovery Inspector uses this information to monitor known and potential threats.

You can connect switches with a mirror port to any of the ports except the management port. Deep Discovery Inspector uses these ports as listening ports and will not interrupt traffic handled by the switches.

For details on how to access the Preconfiguration Console, see the Preconfiguration chapter in the Installation and Deployment Guide.