Device owner identified using a MAC address

You want to identify the identity of the end user of a machine based on a MAC address.

Data required

- **DHCP data**

Procedure

1. Gather the inputs, for example, you might need to identify the user registered to MAC address A4:C9:45:0F:DB.
2. Set the search time range to the average period which users have to register devices. Start small and expand the time range if needed.
3. Run the following search. You can optimize it by specifying an index and adjusting the time range.

   This sample search uses [Cisco Identity Services](https://www.cisco.com/c/en/us/products/collateral/security/cisco-identity-services/index.html) data. You can replace this source with any other identity and account data used in your organization.

   ```
   sourcetype=cisco:ise:syslog
   EndPointMacAddress=A4:C9:45:0F:DB
   user=* 
   eventtype='cisco-ise-passed-authentication'
   ```

Search explanation

Here is an explanation of what each part of this search achieves. You can adjust this query based on the specifics of your environment.

<table>
<thead>
<tr>
<th>Splunk Search</th>
<th>Explanation</th>
</tr>
</thead>
<tbody>
<tr>
<td>sourcetype=cisco:ise:syslog</td>
<td>Search only Cisco ISE logs.</td>
</tr>
<tr>
<td>EndPointMacAddress=A4:C9:45:0F:DB</td>
<td>Search for only events where the EndPointMacAddress is A4:C9:45:0F:DB.</td>
</tr>
<tr>
<td>user=*</td>
<td>Search for any user.</td>
</tr>
</tbody>
</table>

The information provided in Splunk Lantern is intended for informational and educational purposes only. All information is provided in good faith, however, Splunk disclaims any and all representations and warranties, express and implied, regarding the information provided, including without limitation any warranties and representations regarding the completeness, adequacy or accuracy of the information. You agree to take full responsibility for the results arising from the use of the information provided.
<table>
<thead>
<tr>
<th>Splunk Search</th>
<th>Explanation</th>
</tr>
</thead>
<tbody>
<tr>
<td>eventtype='cisco-ise-passed-authentication'</td>
<td>Search for only authentication events that were successfully captured.</td>
</tr>
</tbody>
</table>

**Next steps**

This search returns individual Cisco ISE events that are associated with the device you need to identify the owner of. The event information shows the user account associated with the device owner.

Finally, you might be interested in other processes associated with the [Processing DMCA notices](#) use case.