

Creating Splunk 6.3 Knowledge Objects Lab Exercises

There are a number of source types used in these lab exercises. The lab instructions refer to these source types by the types of data they represent:

Туре	Sourcetype	Interesting Fields
AD/DNS	winauthentication_security (corporate network)	<pre>bcg_ip, bcg_workstation, fname, lname, location, rfid, splunk_role</pre>
	WinEventLog:Security (engineering network)	Account_Domain, Account_Name, action, app, Authentication_Package, Type, User
Badge reader	history_access	Address_Description, Department, Device, Email, Event_Description, First_Name, last_Name, Rfid, Username
BI server	sales_entries	AcctCode, CustomerID, TransactionID
Email data	cisco_esa	dcid, icid, mailfrom, mailto, mid
Web appliance data	cisco_wsa_squid	action, bandwidth, cs_method, cs_mime_type, cs_url, cs_username, sc_bytes, sc_http_status, sc_result_code, severity, src_ip, status, url, usage, x_mcafee_virus_name, x_wbrs_score, x_webcat_code_abbr
Online transactions	access_combined	<pre>action, bytes, categoryId, clientip, itemId, JSESSIONID, price, productId, product_name, referer, referer_domain, sale_price, status, user, useragent</pre>
Retail sales	vendor_sales	AcctID, categoryId, product_name, productId, sale_price, Vendor, VendorCity, VendorCountry, VendorID, VendorStateProvince
Web server	linux_secure	<pre>action, app, COMMAND, dest, process, src_city, src_country, src_ip, src_port, user, vendor_action</pre>



Module 2 Lab Exercise: Creating Lookups

Description

In this lab exercise, you create a new automatic lookup that provides additional information for the web appliance data.

Steps

Task 1: Set your name and time zone.

- 1. Click your student ID (455-xxxxxxx) on the navigation bar and select Edit Account.
- 2. In the **Full Name** field, enter your name.
- 3. From the **Time zone** menu, select your local time zone.
- 4. Un-check Restart backgrounded jobs.
- 5. Click Save.
- 6. Click the splunk> logo at the top left of the window to return to the Search & Reporting app.

Task 2: Search the web appliance data.

- 1. Search the web appliance data [sourcetype=cisco wsa squid] over the last 24 hours
- 2. Examine the fields in the fields sidebar. In the next task, you will create an automatic lookup to add the department and location fields to the results.

Task 3: Create an automatic lookup definition.

- 3. Navigate to: Settings > Lookups > Automatic lookups
- Click New
- 5. Create the automatic lookup with these values:

Destination app: search

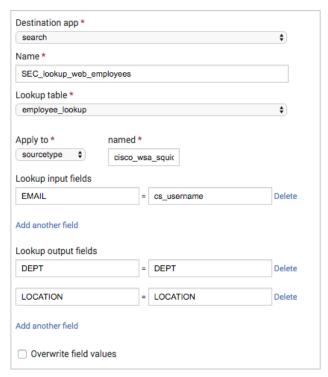
Name: SEC_lookup_web_employees

Lookup table: employee_lookup
Apply to: sourcetype
named: cisco_wsa_squid
Lookup input fields: EMAIL = cs_username

Lookup output fields: DEPT = DEPT

LOCATION = LOCATION





Click Save.

Task 4: Search the web appliance data to verify the automatic lookup is working.

- 7. Search sourcetype=cisco wsa squid over the Last 24 hours.
- 8. In the fields sidebar, click the **DEPT**, and **LOCATION** fields to examine the field values.