

## 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:

Type	Sourcetype	Interesting Fields
AD/DNS	winauthentication_security (corporate network)	bcg_ip, bcg_workstation, fname, lname, location, rfid, splunk_role
	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	action, bytes, categoryId, clientip, itemId, JSESSIONID, price, productId, product_name, referer, referer_domain, sale_price, status, user, useragent
Retail sales	vendor_sales	AcctID, categoryId, product_name, productId, sale_price, Vendor, VendorCity, VendorCountry, VendorID, VendorStateProvince
Web server	linux_secure	action, app, COMMAND, dest, process, src_city, src_country, src_ip, src_port, user, vendor_action

## 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-xxxxxx) 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**
4. Click **New**.
5. Create the automatic lookup with these values:

<b>Destination app:</b>	<b>search</b>
<b>Name:</b>	<b>SEC_lookup_web_employees</b>
<b>Lookup table:</b>	<b>employee_lookup</b>
<b>Apply to:</b>	<b>sourcetype</b>
<b>named:</b>	<b>cisco_wsa_squid</b>
<b>Lookup input fields:</b>	<b>EMAIL = cs_username</b>
<b>Lookup output fields:</b>	<b>DEPT = DEPT</b>
	<b>LOCATION = LOCATION</b>

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 [Delete](#)

[Add another field](#)

Lookup output fields

DEPT = DEPT [Delete](#)

LOCATION = LOCATION [Delete](#)

[Add another field](#)

☐ Overwrite field values

- Click **Save**.

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

- Search `sourcetype=cisco_wsa_squid` over the **Last 24 hours**.
- In the fields sidebar, click the **DEPT**, and **LOCATION** fields to examine the field values.