



okta

# Configure Universal Logout with Identity Threat Protection

Lab Guide

---

Version 2024.10

Copyright 2024 Okta, Inc. All rights reserved.

Window captures and dialog box sample views are the copyright of their respective owners.

Use of this user documentation is subject to the terms and conditions of the applicable End-User License Agreement.

**Disclaimer: Use of fictitious information**

The example companies, organizations, domain names, email addresses, people, and events depicted herein are fictitious. No association with any real company, organization, domain name, email address, person, or event is intended or should be inferred.

# Table of contents

<b>Background</b>	<b>4</b>
Challenges	4
Key Concepts	4
<b>Lab: Access the lab environment</b>	<b>5</b>
Sign in to your Okta training org	5
<b>Lab: Configure Universal Logout for Session-Influenced Risk</b>	<b>6</b>
Configure Entity Risk Policy for Session-influenced user risk	6
Test the session hijacking scenario	6
Confirm entity risk evaluation and response in System Logs	8
<b>Lab: Configure Automated Security Response for Admin-Reported Risk</b>	<b>10</b>
Configure an Entity Risk Policy to trigger Universal Logout for high-risk events	10
Test the Entity Risk Policy	10
Confirm entity risk and response in System Logs	11
<b>Lab: Create a Delegated Workflow for Universal Logout and Notification</b>	<b>12</b>
Authorize API Scopes for Okta Workflows	12
Create a Connection to Okta in Okta Workflows	12
Import the Helper flow	14
Create a delegated Workflow	15
Edit Entity Risk policy for Session-influenced user risk	16
Test the session hijacking scenario	17
Check Execution Results and Notification	18

## Background

### Challenges

Given the recent surge in session hijacking and credential stuffing attacks, Okta has prioritized the implementation of Okta Identity Threat Protection (ITP). As Security Administrator, you'll be responsible for fortifying the company's defenses through improved user session management and threat detection and response.

### Key Concepts

ITP is a security solution designed to protect your organization from attacks targeting identities and identity infrastructure. ITP continuously evaluates a user's session and access to resources using a machine learning-powered Risk Engine that performs ongoing risk assessments. It allows you to configure responses to threats based on risk level, such as:

- Requiring MFA
- Initiating universal logout
- Terminating individual sessions
- Triggering predefined threat response workflows

The labs in this guide focus on these key features of ITP:

- **Universal Logout**

This is an automated security response that terminates active user sessions across all integrated applications when a session violation or elevated risk is detected. It helps ensure that compromised sessions are promptly ended, reducing the risk of unauthorized access.

- **Entity Risk Policy**

Entity Risk Policy allows you to set up automated responses to various types of user account risks. It operates based on:

- **Entity Risk:** The probability of a user account being compromised, assessed across devices, sessions, and applications.
- **Risk Detections:** Specific types of security threats or suspicious activities identified by ITP.




In the labs, you'll configure Entity Risk Policies to trigger actions like Universal Logout or custom workflows in response to different risk scenarios.

## Lab: Access the lab environment

### Objective

Sign in to your Okta training org.

### Sign in to your Okta training org

1. View the credentials for the tenants used in this course.
  - a. From the right side of the workspace, select the **arrow** to open the side panel.
  - b. From the Credentials tab, locate the Okta training org credentials for this lab.
2. Sign in to the Okta training org.
  - a. From the workspace, open a Chrome browser window.
  - b. From the side panel, select **Paste to VM**  for the **Link** field to paste the org URL.  
**Note:** Before selecting paste, ensure the field you are pasting into has focus.
  - c. From the Chrome browser window, place the cursor in the URL and select **Enter**.
  - d. From the side panel, select **Paste to VM**  for the **Login** field to paste the org username.
  - e. From the Chrome browser window, select **Next**.
  - f. From the side panel, select **Paste to VM**  for the **Password** field to paste the org password.
  - g. From the Chrome browser window, select **Verify**.
  - h. Select the **arrow** to close the side panel.
3. From the End-User Dashboard, select **Admin** to open the Admin Console.

**Note:** This user has Super Administrator permissions.

End of lab

## Lab: Configure Universal Logout for Session-Influenced Risk

### Objective

Configure Universal Logout to automatically log users out of applications when their risk is elevated in Okta.

### Scenario

Okta's security team detected potential session hijacking on the Okta End-user Dashboard. A compromised session could lead to unauthorized access, security setting changes, and data exposure. As the administrator, your task is to implement Universal Logout to quickly terminate suspicious sessions across all integrated applications and mitigate these risks.

### Configure Entity Risk Policy for Session-influenced user risk

1. In the Admin Console, go to **Security > Entity Risk Policy**.
2. Select **Add rule**.
3. For the name, enter **Session-influenced risk response**.
4. Configure the rule to take logout and revoke token action when a session-influenced risk is detected.
  - a. Set the IF condition.
    - i. For the Detection setting, select **Include at least one of the following detections**.
    - ii. In the pop-up conditional field, select **Session Influenced User Risk**.
  - b. For the THEN Take this action option, select **Logout and revoke tokens**.
5. Select **Save**.
6. Sign out from the oktatraining account.

### Test the session hijacking scenario

1. Sign in to the End-User Dashboard as Fitz Sugge.
  - Username: **fitz.sugge**
  - Password: **Tra!nme4321**
2. Open Chrome Developer Tools.
  - a. Select the three-dot Chrome menu in the top-right corner.
  - b. From the dropdown menu, select **More tools > Developer tools**.
3. Access Cookies.
  - a. In the Developer Tools panel, select the double-arrow icon (if needed) and then select the **Application** tab.
  - b. In the left-hand panel under Storage, expand the **Cookies** section.

- c. Select your org's domain name from the list.
4. Locate and copy the session's idx cookie.
  - a. In the main panel, from the cookie list, select **idx**.
  - b. Double-click the value shown in the Cookie Value section.
  - c. Once selected, right-click and choose **Copy** to copy the value.

The screenshot shows the Chrome DevTools Application tab with the 'Cookies' section expanded. The 'idx' cookie is selected, and its value is displayed in the 'Cookie Value' section.

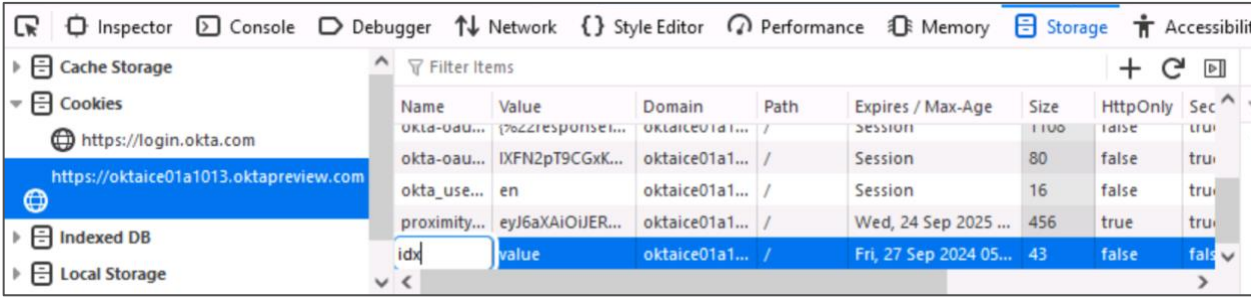
Name	Value	D	P	E	S	H	S	S	P	C	P
DT	DI110X1xgn2T...	o..	/	2...	2...	✓	✓	N..			M.
JSESS...	34B40D7D4B...	o..	/	S...	4...	✓	✓				M.
autol...	true	o..	/	S...	2...						M.
endu...	2	o..	/	2...	1...		✓	N..			M.
idx	eyJ6aXAiOiJE...	o..	/	S...	1...	✓	✓	N..			M.
ln	fitz.sugge	o..	/	2...	1...		✓				M.
luf_1...	eyJ6aXAiOiJE...	o..	/	2...	4...	✓	✓	N..			M.
luf_2...	eyJ6aXAiOiJE...	o..	/	2...	4...	✓	✓	N..			M.
okta-...	K6kMVW8uY...	o..	/	S...	8...		✓	N..			M.
okta-...	{%22respons...	o..	/	S...	1...		✓	N..			M.
okta-...	4rTuPLtY74wf...	o..	/	S...	8...		✓	N..			M.
okta_...	en	o..	/	S...	1...		✓				M.
proxi...	eyJ6aXAiOiJE...	o..	/	2...	4...	✓	✓	N..			M.
proxi...	eyJ6aXAiOiJE...	o..	/	2...	4...	✓	✓	N..			M.
srefre...	17266145905...	o..	/	S...	2...		✓				M.
t	default	o..	/	S...	8						M.

**Cookie Value** ☐ Show URL-decoded

eyJ6aXAiOiJERUYLCjZ2ZXliOiIiYXpYXMiOiJlbmNyeXB0aW9ua2V5liwib2IkljoiMD8vZ3ZyY2tuMkpPdkticjQxZDciLCJlbmMiOiJBMjU2R0NNIiwiaWVwbnljoiZGlyliwieHNpZCI6ImIkeGIGdmQ5U21JU1hPRURNX3RKQTA3WIEifQ..noyP-SFRmF-QY5Zy.u89iPqymwRjjVRL\_cDCrRzHFwvN5RwJ17\_3JMqFhc8w4-ASa0NSnsr3h-ytjW4m0-9dvWih5MZET4EsjFNf1LQeg7eZ-TWJaQM3uk5Cdg4JB3t93Ce4vBgmurDMUVSE6kP5-6EyHCduoKZFJ0Qr8lGHg3G9cZXIbqKwAVpWvRBh11jDuKDAa6suUmy4R3rFShWsK9Sp8wiE\_GNI4VOcfaf5nd8vMT76PXySaotD0i5O1BNQrZ15h--XMav8IMsTHMznG6\_P5rT85NTA3NIV8ZZPgvD-rs1SJ3Qi1Sz7H260h9\_KnU60FMObBLS0wfu32ScIOPf9J7Uvh-PB6\_cPUZo9

5. In your workspace, launch a Firefox browser window.
6. From the side panel, select **Paste to VM** for the **Link** field to paste the org URL.
7. Configure Browsec VPN to simulate access from a different IP address.
  - a. In Firefox toolbar, select the Extensions icon in the top-right corner.
  - b. Select **Browsec VPN – Free VPN for Firefox**.
  - c. Select **Start VPN** to initiate the VPN connection.

**Note:** You can select **Change** to switch to a different geographical location for your VPN connection.

8. Access Cookies.
    - a. With Browsec VPN active, select the application menu icon (three horizontal lines) in the top-right corner.
    - b. From the dropdown menu, select **More tools > Web Developer Tools**.
    - c. In the Web Developer Tools panel, select the **Storage** tab at the top.
    - d. In the left panel, expand **Cookies**.
    - e. Select your org's domain name from the list.
  9. Add the idx cookie.
    - a. In the main panel where the cookies are listed, right-click and select **Add Item** from the context menu.
    - b. Verify that a new row appears at the bottom of the list of cookies.
    - c. Double-click the **Name** field and enter **idx**.
- 
- | Name         | Value            | Domain         | Path | Expires / Max-Age      | Size | HttpOnly | Secure |
|--------------|------------------|----------------|------|------------------------|------|----------|--------|
| okta-oau...  | 7%22response...  | oktaice01a1... | /    | Session                | 1100 | true     | true   |
| okta-oau...  | IXFN2pT9CGxK...  | oktaice01a1... | /    | Session                | 80   | false    | true   |
| okta_use...  | en               | oktaice01a1... | /    | Session                | 16   | false    | true   |
| proximity... | eyJ6aXAiOiJER... | oktaice01a1... | /    | Wed, 24 Sep 2025 ...   | 456  | true     | true   |
| idx          | value            | oktaice01a1... | /    | Fri, 27 Sep 2024 05... | 43   | false    | false  |
- d. Double-click the **Value** field and paste the previously copied value of the idx cookie.
  - e. Press **Enter** to save the cookie.
10. Reload the page and verify that you see the Session revoked message.
11. Back in your Chrome, reload the end-user dashboard.
12. Verify that Fitz is logged out and prompted to log in again (indicating the session was successfully terminated).

## Confirm entity risk evaluation and response in System Logs

1. Sign in to the Okta org as **oktatraining**.
2. From the End-User Dashboard, select **Admin** to open the Admin Console.
3. From the Admin Console, go to **Reports > System Log**.
4. In the search field, enter `user.session.context.change` to confirm the event is triggered when Okta identifies a change in a user's session context.
5. You can also find the following events after a change in the user session context:



Event	Corresponding event type
Okta detects user risk.	<code>user.risk.detect</code>
Okta evaluates the entity risk policy (against the Session-influenced user risk rule)	<code>policy.entity_risk.evaluate</code>
Okta invokes an action.	<code>policy.entity_risk.action</code>
Okta invokes Universal Logout for session violations	<code>user.session.end</code>
Okta invokes Universal Logout against an app instance	<code>user.authentication.universal_logout</code>

End of lab

## Lab: Configure Automated Security Response for Admin-Reported Risk

### Objective

Set up an automated security response to trigger a Universal Logout when an admin reports a risk.

### Scenario

Okta wants to ensure swift action in response to high-risk situations identified by admins. By configuring automated security responses, you'll enable immediate actions, such as Universal Logout, to protect sensitive data.

### Configure an Entity Risk Policy to trigger Universal Logout for high-risk events

1. In the Admin Console, go to **Security > Entity Risk Policy**.
2. Select **Add rule**.
3. For the Name, enter **Admin-flagged risk response**.
4. Configure the rule to take logout and revoke token action when an admin-reported user risk is detected.
  - a. Set the IF condition.
    - i. For the User's group membership includes setting, select **At least one of the following groups:**.
    - ii. In the pop-up conditional field, enter and select **Sales**.
    - iii. For the Detection setting, select **Include at least one of the following detections:**.
    - iv. In the pop-up conditional field, select **Admin Reported User Risk**.
    - v. For the Entity risk level setting, select **High**.
  - b. For the THEN Take this action setting, select **Logout and revoke tokens**.
5. Select **Save**.

### Test the Entity Risk Policy

1. Select the Chrome menu in the top-right corner of your Chrome browser.
2. Select **New Incognito window**.
3. Sign in to the End-User Dashboard as Mayer Hay.
  - Username: **mayer.hay**
  - Password: **Tra!nme4321**
4. Elevate the risk level of the test user.
  - a. Back in the Admin Console of your Chrome browser, go to **Directory > People**.
  - b. Select **Mayer Hay**.

- c. Select **More Actions > Elevate entity risk level**.
- d. Select **Yes, elevate risk level**.
5. In the Incognito window, refresh Mayer's end-user dashboard.
6. Verify that you see a "Session Revoked" message.
7. Close the Incognito window.

## Confirm entity risk and response in System Logs

1. In the Admin Console, go to **Reports > System Log**.
2. You can find the following events are recorded:

Event	Corresponding event type
Okta detects user risk.	<code>user.risk.detect</code>
Okta evaluates the entity risk policy (against the Admin-flagged risk response rule)	<code>policy.entity_risk.evaluate</code>
Okta invokes an action.	<code>policy.entity_risk.action</code>
Okta invokes Universal Logout for session violations	<code>user.session.end</code>
Okta invokes Universal Logout against an app instance	<code>user.authentication.universal_logout</code>

## Lab: Create a Delegated Workflow for Universal Logout and Notification

### Objective

Configure a delegated Okta workflow for universal logout and automated email notifications in response to session risks or violations.

### Scenario

OktaInc wants to strengthen its response to potential session hijacking and risk violations. By configuring a delegated workflow, you'll enable automated universal logout for compromised sessions and send notifications to administrators, ensuring swift action and enhanced security.

### Authorize API Scopes for Okta Workflows

Authorizes the necessary API scopes to allow the Okta Workflows to call Okta APIs for managing universal logout.

1. In the Okta Admin console, go to **Applications > Applications**.
2. Select **Okta Workflows OAuth**.
3. In the Okta Workflows OAuth app page, select the **Okta API Scopes** tab.
4. Select **Grant** for the following scopes:
  - **okta.universalLogout.manage**
  - **okta.userRisk.manage**
5. In the warning message that appears, select **Grant Scope** to confirm.

### Create a Connection to Okta in Okta Workflows

1. In the Okta Admin Console, go to **Workflow > Workflows console**.
2. In the Okta Workflows Console (opened in a new browser tab), select **Connections** in the navigation menu at the top.
3. Select **New Connection**.
4. In the search box, type **Okta**, then select **Okta** from the search results.
5. Retrieve Client ID and Client Secret from the Okta Admin Console:
  - a. Switch back to the Okta Admin Console.
  - b. In the Okta Workflows OAuth app page, select the **Authentication** tab.
  - c. In the Sign-on methods section, locate the Client ID and Client Secret.

The screenshot shows the 'Okta Workflows OAuth' console. The 'Authentication' tab is selected. Under 'Sign-on settings', the 'Sign-on methods' section shows 'OpenID Connect' as the selected method. The 'Client ID' field contains a long alphanumeric string, and the 'Client secret' field contains a masked string. To the right, the 'About' section explains that OpenID Connect allows users to sign on to applications using the OpenID Connect protocol. Below this, the 'Application Username' section explains that users can choose a format to use as the default username value when assigning the application to users. If 'None' is selected, users will be prompted to enter the username manually.

6. Enter new connection details:

- a. Return to the **New Connection** window in the Okta Workflows Console.
- b. Under the General tab, make the following configurations:

Field	Value
Name	Keep the default value.
Client ID	Copy the Client ID from the OAuth app in the Admin Console and paste it here.
Client Secret	Copy the Client Secret from the OAuth app and paste it here.
Domain	Enter your Okta domain without the "https://" or "-admin" part (e.g., oktaice#####.oktapreview.com).  <b>Tip:</b> You can copy the domain name from the credential pane and remove the https://.

- c. Select the Permissions tab, and make the following configurations:
  - i. Select **Customize scopes (advanced)**.

- ii. Scroll to the bottom, in the **Manually add scopes** field, enter **okta.universalLogout.manage**  
**okta.userRisk.manage**

**Note:** Make sure there is a space in between each scope.

**Manually add scopes**

If the scope(s) you need do not appear in the table above, you can enter them here. Separate multiple scopes with a space.

okta.universalLogout.manage okta.userRisk.manage
 ✓

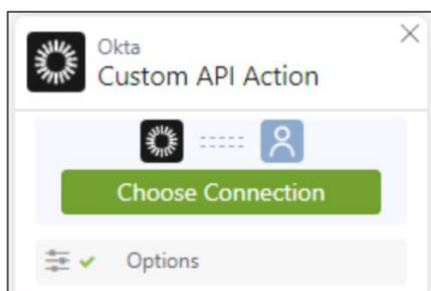
Add

- iii. Select **Add**.
- d. Select **Create**.
- e. Verify that the Okta connection displays in the Workflows console.

## Import the Helper flow

The helper flow makes a custom API call to the [Global Token Revocation](#) endpoint to trigger Universal Logout.

1. In the navigation menu at the top, select the **Flows** tab.
2. In the Folders pane, select the three dots (more options) next to Default Folder.
3. From the dropdown menu, select **Import**.
4. Navigate to the folder C:\Adv\_Sec\Flows.
5. Locate the **universalLogout.flow** file and import it.
6. In the main pane, select the **Universal Logout** helper flow.
7. Select Okta connection.
  - a. In the flow builder, locate the Okta Custom API Action card
  - b. Select **Choose Connection**.
  - c. Select **Okta**.



8. Select **Flow is OFF** and toggle the flow to **ON**.

9. Select **Save**.
10. In the top-left corner, select **Default Folder**.

## Create a delegated Workflow

1. In Default Folder, select **New flow**.
2. Rename the flow.
  - a. Next to Unnamed, select the **pencil** icon.
  - b. Enter **Universal logout and Alert**.
  - c. Select **Save**.
3. Create the event.
  - a. Select **Add event**.
  - b. Under Built-in triggers, select **Delegated Flow**.
4. Call the Helper flow.
  - a. Select **Add function** in the next step of your flow.
  - b. From the list of Most Popular functions, select **Call Flow**.
  - c. In the Call Flow card, select **Choose Flow**.
  - d. Select **Default Folder > Universal Logout**.
  - e. Select **Choose**.
  - f. Select and drag the **Okta User ID** from the Delegated Flow card and drop it into the **User ID** field in the Call Flow card.
5. Add and configure a Compose Text Action
  - a. Select **Add function** in the next step of your flow.
  - b. From the list of Most Popular functions, select **Compose**.
  - c. In the Compose action card, write the notification message, such as:  
The following user ID's Okta session triggered a risk policy,  
and the session was revoked to mitigate the risk.
  - d. Drag the **Okta User ID** from the Delegated Flow card and drop it below your composed message in the Compose action card.  
**Note:** This dynamically inserts the user ID into the message.
6. Add an API Connector Action.
  - a. Select **Add app action** in the next step of your flow.
  - b. In the search box, type **API** and then select **API Connector** from the search results.
  - c. Select **Post** from the list of methods.
  - d. Select **+ New Connection**.
  - e. In the New Connection window, select **None** for Auth Type.
  - f. Select **Create**.

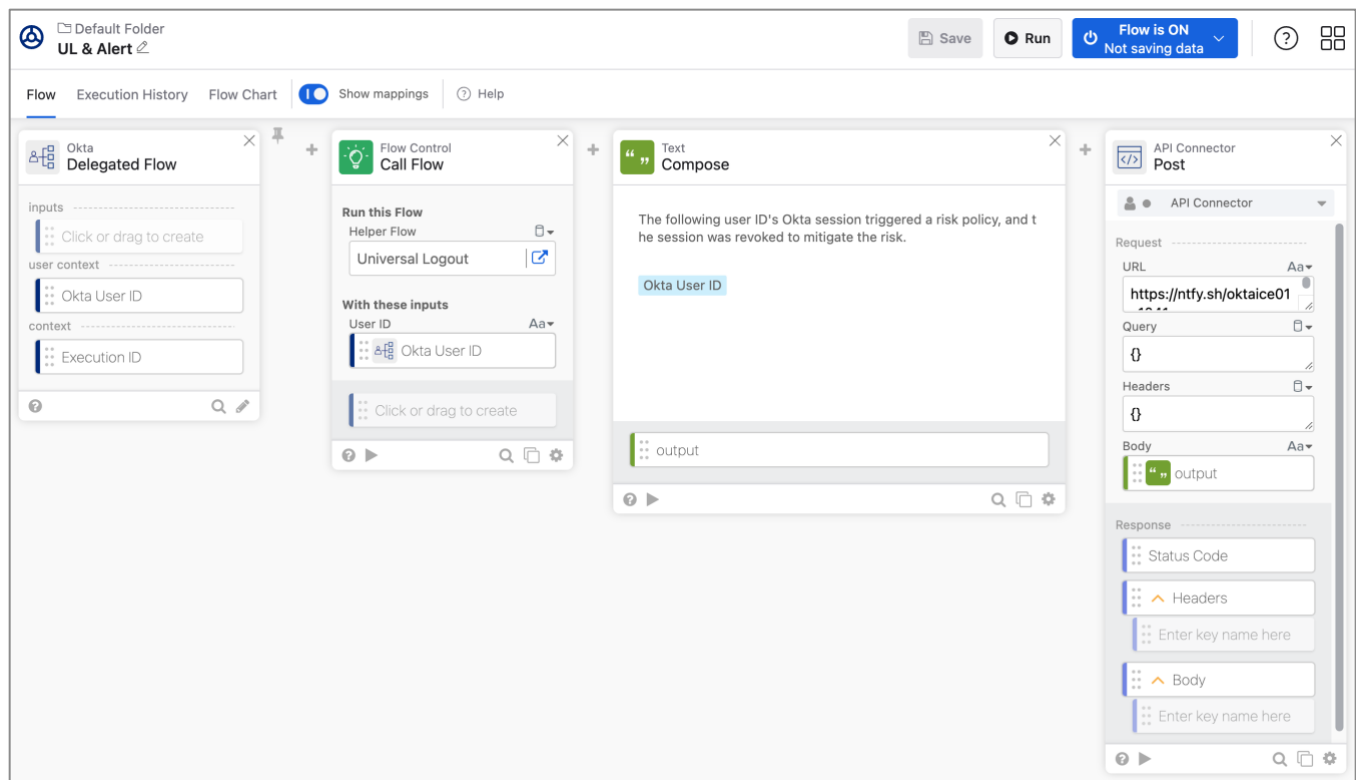
## 7. Subscribe a topic in ntfy.sh.

**Note:** ntfy.sh is a lightweight publish-subscribe (pub-sub) service for sending push notifications to your phone or desktop.

- Open a new browser tab, enter <https://ntfy.sh/app>
- Select **Subscribe to a topic**.
- Enter your domain name – a unique value, such as oktaice01a0000.
- Select **Subscribe**.
- Copy the value: **ntfy.sh/<your domain name>**.

## 8. Configure notification in the API Connector Action.

- Return to the Workflow console.
- In the API Connector Post card, paste the value in the URL field and add **https://** so the full URL reads:  
`https://ntfy.sh/<your domain name>`
- Drag the output from the Compose action and drop it into the Body field.

9. When your flow is complete, select **Save**.10. Select **Flow is OFF** and toggle the flow to **ON**.

## Edit Entity Risk policy for Session-influenced user risk

1. In the Admin Console, go to **Security > Entity Risk Policy**.



2. Update the rule to change the action to Run a Workflow.
  - a. Next to the Session-Influenced Risk Response rule, select **Actions > Edit**.
  - b. For the THEN Take this action setting, select **Run a Workflow**.
  - c. In the Workflow triggered by action field, select **Universal logout and Alert**.
3. Select **Save**.
4. Sign out from the oktatraining account.

## Test the session hijacking scenario

1. Sign in to the End-User Dashboard as Wells Betonia.
  - Username: **Wells.Betonia**
  - Password: **Tra!nme4321**
2. Open Chrome Developer Tools.
  - a. Select the three-dot Chrome menu in the top-right corner.
  - b. From the dropdown menu, select **More tools > Developer tools**.
3. Access Cookies.
  - a. In the Developer Tools panel, select the **Application** tab at the top.
  - b. In the left-hand panel under Storage, expand the **Cookies** section.
  - c. Select your org's domain name.
4. Locate and copy the session's idx cookie
  - a. In the main panel, from the cookie list, select **idx**.
  - b. Double-click the value shown in the Cookie Value section.
  - c. Once selected, right-click and choose **Copy** to copy the value.
5. From your Firefox browser window, enter your org URL.
6. Verify Browsec VPN is still active.
7. Access cookies.
  - a. In the top-right corner, select the application menu icon (three horizontal lines).
  - b. From the dropdown menu, select **More tools > Web Developer Tools**.
  - c. In the Web Developer Tools panel, select the **Storage** tab at the top.
  - d. In the left panel, expand **Cookies**.
  - e. Select your org's domain name from the list.
8. Edit the existing IDX cookie if you have one. If not, add a new cookie.
 

**Note:** See Lab 1, Test the Session Hijacking Scenario, Step 9 for instructions on adding a new cookie.
9. Reload the sign-in page and verify that you see the Session revoked message.
10. Back in your Chrome, reload the end-user dashboard.
11. Verify that Wells is signed out and prompted to sign in again (indicating the session was successfully terminated).

## Check Execution Results and Notification

1. In Okta Workflows Console, select the **Execution History** tab in the flow builder.
2. Confirm that the workflow completed successfully.
3. Go to the ntfy.sh browser tab, select your subscribed topic.
4. Verify that you received the alert message composed in the Compose action.