Welcome to the hands-on portion of this exam! Below are the login information and credentials you will need to take Part II You will use the same Admin username and Admin password for Org1 and Org2 Please review the Part II Info tab for further information

Org1 URL:	https://org1-ocapp78bq.oktapreview.com
Org2 URL:	https://org2-ocapp78bq.oktapreview.com
Admin Username:	user.admin@oktacertified.com
Admin Password:	Testme321!

Download File

Click "Download File" to download the comma-separated values file to your local

drive so that you can import it into your Okta org.

Use-Case 01

1. Importing Users from CSV:
   - Open the downloaded CSV file and import it into the Okta tenant.
   - The file contains 5 users for updates and the rest are new users.
   - If any issues arise during the import, debug and resolve them accordingly.
2. Creating a Custom User Type:
   - Create a custom user type named '**Custom User Type**'.
   - Add an attribute called '**Custom Attribute**' to this user type.
3. Creating User Groups:
   - Create the following groups:
     - **HR Group**
       - Description: All HR personnel
     - **Marketing Group**
       - Description: All Marketing personnel
4. Automating User Addition to Marketing Group:
   - Implement a group rule named '**Marketing Rule**' to automatically add users to the Marketing Group based on their **department**.
5. Admin Group User Assignment:
   - Manually assign all users to the **Admin Group**.
6. User Login Verification:
   - Activate an user in '**Staged**' status and Log in with thatD user credential into Org1 and verify if the login is successful.

First Name	Last Name	Username/Email	Password
Anna	Wu	anna.wu@oktacertified.com	Testme321!

1. Configure a custom SAML 2.0 integration between Org1 (IdP) and Org2 (SP). Do **NOT** use the Okta Integration Network (OIN) to perform your integration. Name the integration **Engapp**.

2. Set up **FirstName**, **LastName**, and **Email** mapping from Org1 to Org2.

3. Use expression language to combine **firstName** and **lastName** in Org1 into a new attribute called **empName** and has the format 'lastName firstName'. For example, firstName: Anna and lastName: Wu should become empName: Wu Anna.

4. Map **empName** in Org1 to **DisplayName** in Org2.

5. Assign the **Everyone** group to the **Engapp** application. Sign into Org1 as Anna Wu using the credentials in the table. Verify that Anna can access Org2 using the **Engapp** application.

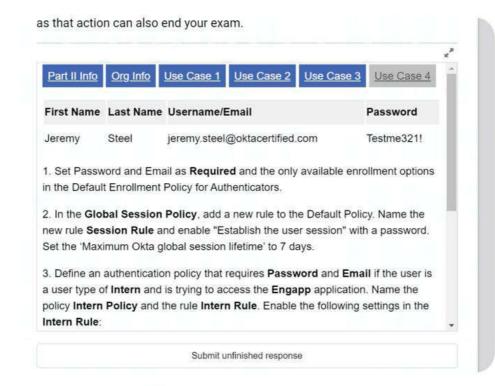| First Name	Last Name	Username/Email	Password
Fiona	Boots	fiona.boots@oktacertified.com	Testme321!

1. As User Admin create a custom Admin role that can "manage users and groups". Name this role **Management Admin**.

2. Create a resource set called **Manage Users and Groups**. Assign the resource type to Users and enable the "constrain to all users" option. Add a second resource type to groups and enable the "Constrain to all groups" option.

3. Assign the new Management Admin role to **Fiona Boots**

4. Sign in as Fiona using the credentials in the table and suspend **Yousef Patel**.

Okta Hands On Administrator

Okta/Workforce Identity

Good day, I'm having trouble with use case 4 (see images). I've followed all the steps but I'm still getting 50% over 100%. Can anyone help me?

as that action can also end your exam.

Part II Info	Org Info	Use Case 1	Use Case 2	Use Case 3	Use Case 4

First Name	Last Name	Username/Email	Password
Jeremy	Steel	jeremy.steel@oktacertified.com	Testme321!

1. Set Password and Email as **Required** and the only available enrollment options in the Default Enrollment Policy for Authenticators.

2. In the **Global Session Policy**, add a new rule to the Default Policy. Name the new rule **Session Rule** and enable "Establish the user session" with a password. Set the 'Maximum Okta global session lifetime' to 7 days.

3. Define an authentication policy that requires **Password** and **Email** if the user is a user type of **Intern** and is trying to access the **Engapp** application. Name the policy **Intern Policy** and the rule **Intern Rule**. Enable the following settings in the **Intern Rule**:

Submit unfinished response

a user type of **Intern** and is trying to access the **Engapp** application. Name the policy **Intern Policy** and the rule **Intern Rule**. Enable the following settings in the **Intern Rule**:

- And Prompt for password authentication: When an Okta global session doesn't exist
- And Prompt for all other factors: Every time user signs in to resource

4. If you can, use a personal email address to receive the Email verification code. Otherwise, if you are taking this exam on a device that is locked down, you may have to use a work email address. Edit Jeremy Steele's Okta Profile and set his primary email to the email address that you are using for this step.

5. Log in as **Jeremy Steel** to verify that you are prompted for **Email verification** upon clicking the **Engapp** tile from the Okta dashboard in Org1.

6. Complete the login by accessing the email with Jeremy's verification code.

Add a comment