Revoking a User's App Privilege When User is Assigned via Group Membership

Statement:

Okta is recommending enterprises to assign user's to group for application permissions.

Question:

How does YouAttest revoke a user in this scenario?

Answer:

YouAttest provides **Group Audits** (See Use Case #1 below) that allows administrators and reviewers to certify or revoke users from groups. If revoked from a group, all applications assigned to the user due to that group assignment will automatically be revoked by Okta. This uses Okta's best practices to allow or revoke access using group assignments.

In case of **Application Audits** (See Use Case #2, below) , YouAttest revokes the application access without removing the user from the group. We simply change the scope of the assignment from "group" to "user" and then remove that user from the application. This way, the user remains part of the group, however, that specific application access is removed. For individual assignments, we don't have to make changes in the user's scope.

We accomplish this by leveraging two Okta API endpoints.

1. Update Application Profile for Assigned User

a. This API is used to change user's scope

More information about this API is as follow:

Update application profile for assigned user

POST /api/v1/apps/${applicationId}/users/${userId}

Updates a user's profile for an application

Request parameters

Parameter	Description	Param Type	DataType	Required	Default
applicationId	`id` of an app	URL	String	TRUE	
uid	unique key of a valid User	URL	String	TRUE	
appuser	credentials for app	Body	Application User	FALSE	

Response parameters

Application User with user profile mappings applied

Your request is rejected with a `403 Forbidden` status for applications with the `PUSH_NEW_USERS` or `PUSH_PROFILE_UPDATES` features enabled if the request specifies a value for an attribute that is defined by an application user profile mapping (Universal Directory) and the value for the attribute doesn't match the output of the mapping.

> **Note:** The Okta API currently doesn't support entity tags for conditional updates. It's only safe to fetch the most recent profile with Get assigned user for application, apply your profile update, and then `POST` back the updated profile as long as you are the only user updating a user's application profile.

```
{
  "errorCode": "E0000075",
  "errorSummary": "Cannot modify the firstName attribute because it has a field mapping and profile pu
  "errorLink": "E0000075",
  "errorId": "oaez9dW_WXiR_K-WwaTKhlgBQ",
  "errorCauses": []
}
```

Request example

```
curl -v -X POST \
-H "Accept: application/json" \
-H "Content-Type: application/json" \
-H "Authorization: SSWS ${api_token}" \
-d '{
  "profile": {
```

2. Remove User from Application

a. This API is then called to remove the user from the application

More information about this endpoint is given hereunder

Remove user from application

DELETE /api/v1/apps/${applicationId}/users/${userId}

Removes an assignment for a user from an application

For directories like Active Directory and LDAP, they act as the owner of the user's credential with Okta delegating authentication (DelAuth) to that directory. If this request is made for a user when DelAuth is enabled, then the user will be in a state with no password. You can then reset the user's password.

Important: This is a destructive operation. You can't recover the user's app profile. If the app is enabled for provisioning and configured to deactivate users, the user is also deactivated in the target application.

Request parameters

Parameter	Description	Param Type	DataType	Required	Default
applicationId	`id` of an app	URL	String	TRUE	
sendEmail	Sends a deactivation email to the administrator if `true`. Default value is `false`	Query	Boolean	FALSE	FALSE
uid	unique key of assigned User	URL	String	TRUE	

Response parameters

An empty JSON object `{}`

Request example

```
curl -v -X DELETE \
-H "Accept: application/json" \
-H "Content-Type: application/json" \
-H "Authorization: SSWS ${api_token}" \
"https://${yourOktaDomain}/api/v1/apps/0oad5lTSBOMUBOBVVQSC/users/00ud4tVDDXYVKPXKVLCO?sendEmail=
```