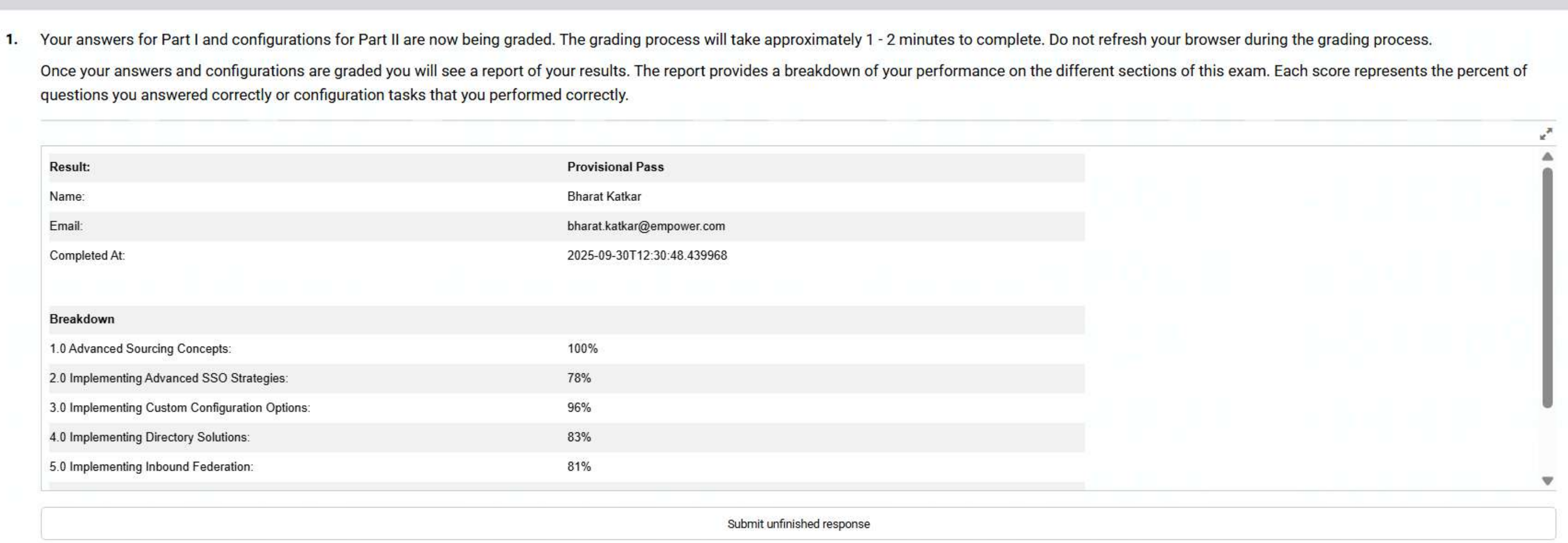
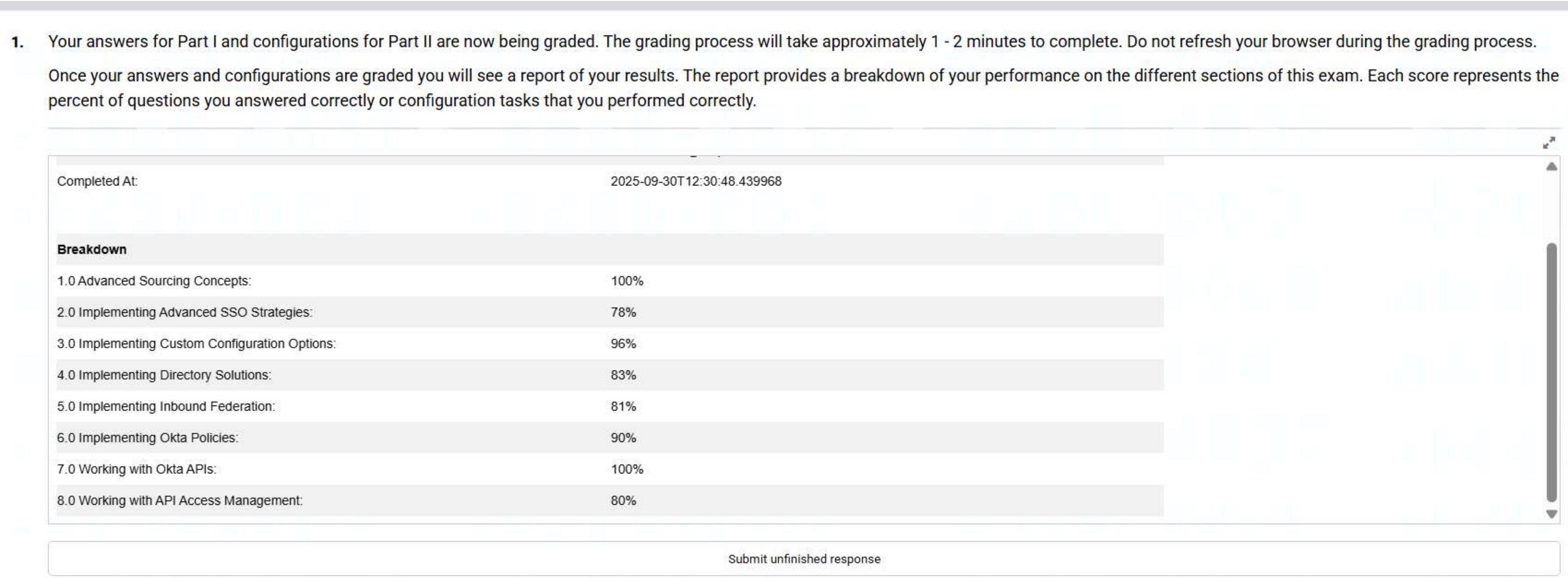


1. Your answers for Part I and configurations for Part II are now being graded. The grading process will take approximately 1 - 2 minutes to complete. Do not refresh your browser during the grading process.

Once your answers and configurations are graded you will see a report of your results. The report provides a breakdown of your performance on the different sections of this exam. Each score represents the percent of questions you answered correctly or configuration tasks that you performed correctly.

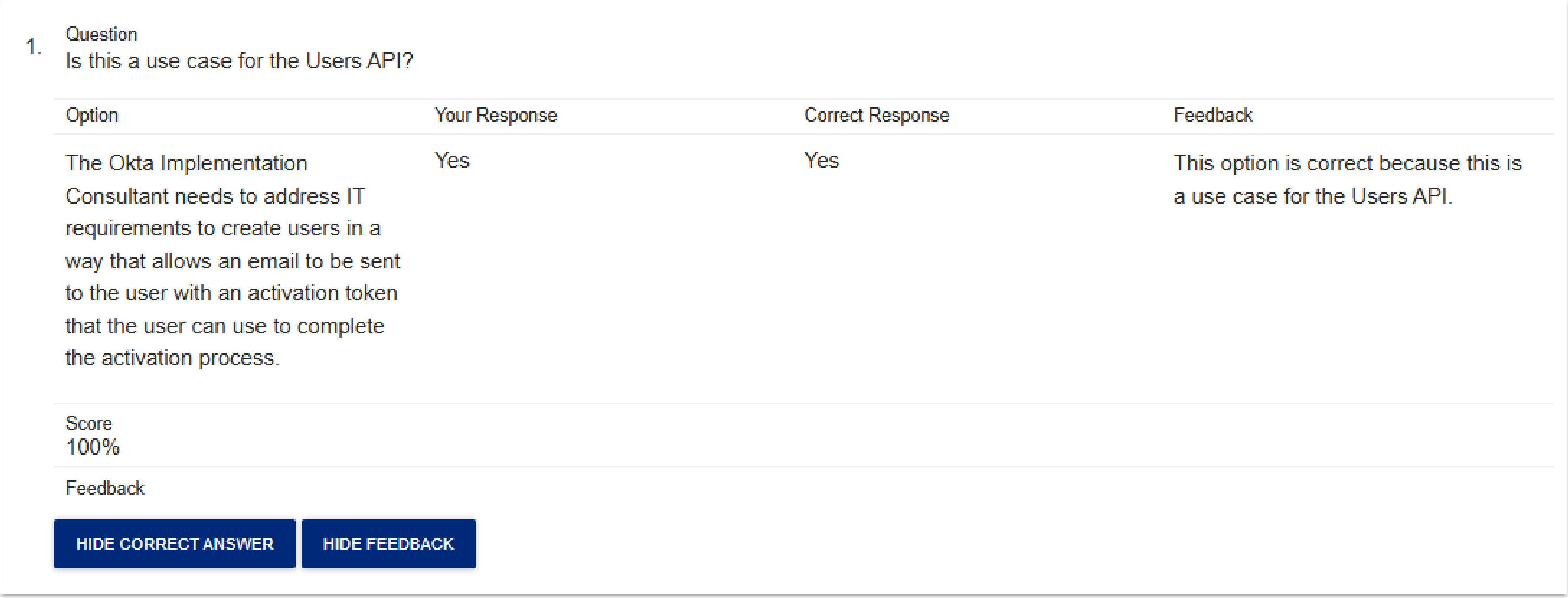
Result:	**Provisional Pass**
Name:	Bharat Katkar
Email:	bharat.katkar@empower.com
Completed At:	2025-09-30T12:30:48.439968
Breakdown	
1.0 Advanced Sourcing Concepts:	100%
2.0 Implementing Advanced SSO Strategies:	78%
3.0 Implementing Custom Configuration Options:	96%
4.0 Implementing Directory Solutions:	83%
5.0 Implementing Inbound Federation:	81%



1. Your answers for Part I and configurations for Part II are now being graded. The grading process will take approximately 1 - 2 minutes to complete. Do not refresh your browser during the grading process.

   Once your answers and configurations are graded you will see a report of your results. The report provides a breakdown of your performance on the different sections of this exam. Each score represents the percent of questions you answered correctly or configuration tasks that you performed correctly.

Completed At:	2025-09-30T12:30:48.439968
Breakdown	
1.0 Advanced Sourcing Concepts:	100%
2.0 Implementing Advanced SSO Strategies:	78%
3.0 Implementing Custom Configuration Options:	96%
4.0 Implementing Directory Solutions:	83%
5.0 Implementing Inbound Federation:	81%
6.0 Implementing Okta Policies:	90%
7.0 Working with Okta APIs:	100%
8.0 Working with API Access Management:	80%



1. Question

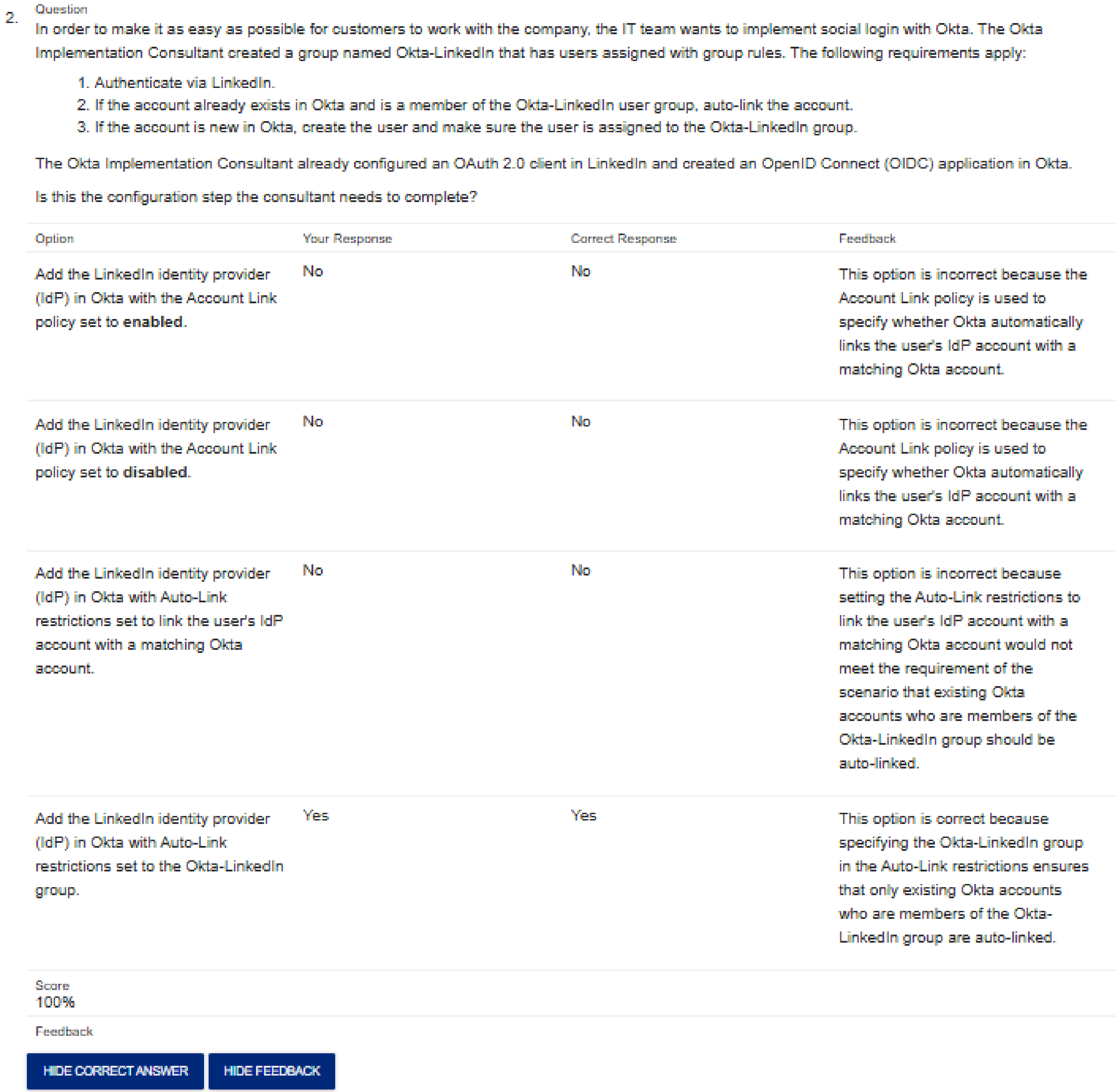
Is this a use case for the Users API?

Option	Your Response	Correct Response	Feedback
The Okta Implementation Consultant needs to address IT requirements to create users in a way that allows an email to be sent to the user with an activation token that the user can use to complete the activation process.	Yes	Yes	This option is correct because this is a use case for the Users API.

Score

100%

Feedback



2. Question

In order to make it as easy as possible for customers to work with the company, the IT team wants to implement social login with Okta. The Okta Implementation Consultant created a group named Okta-LinkedIn that has users assigned with group rules. The following requirements apply:

1. Authenticate via LinkedIn.
2. If the account already exists in Okta and is a member of the Okta-LinkedIn user group, auto-link the account.
3. If the account is new in Okta, create the user and make sure the user is assigned to the Okta-LinkedIn group.

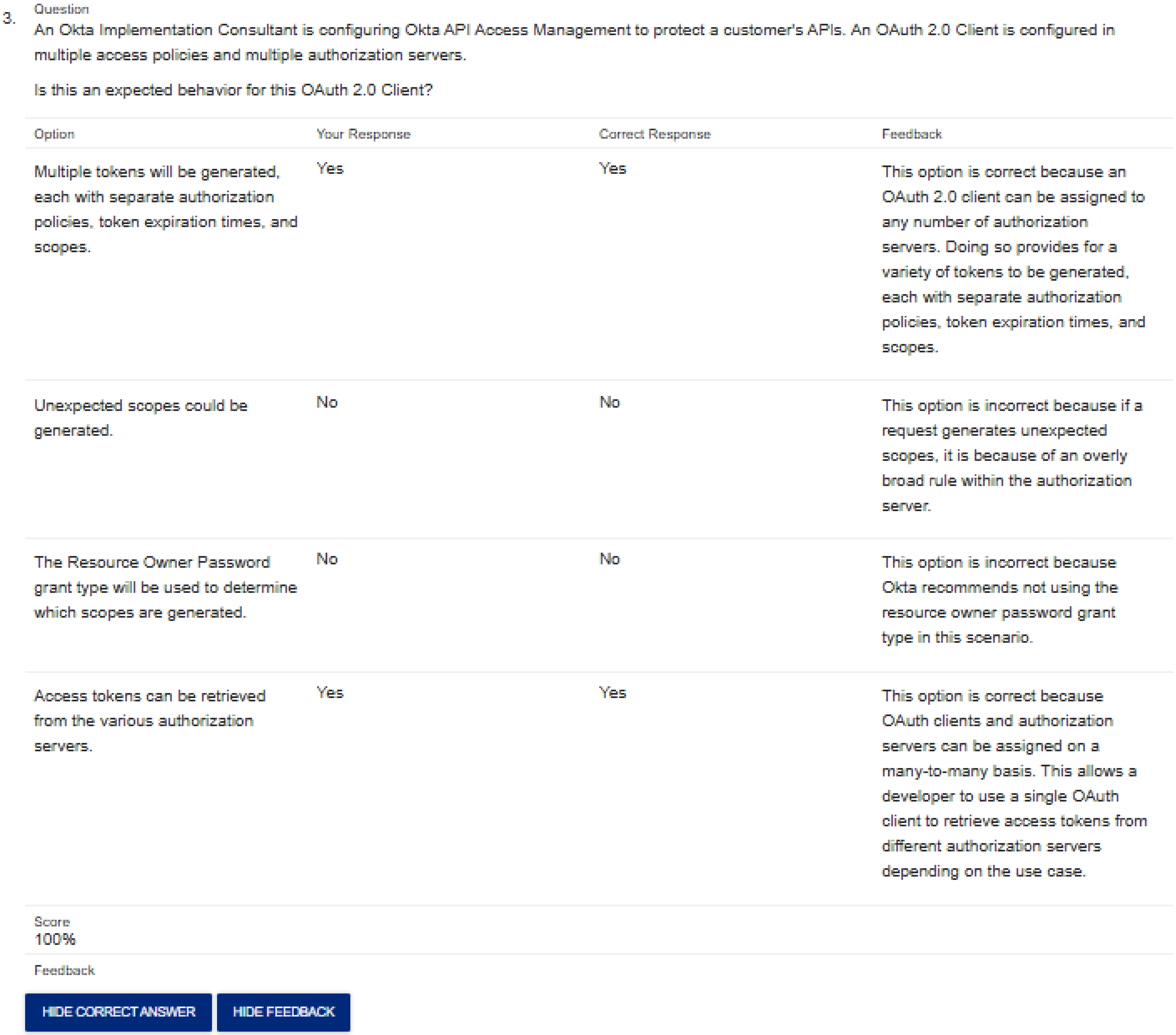
The Okta Implementation Consultant already configured an OAuth 2.0 client in LinkedIn and created an OpenID Connect (OIDC) application in Okta.

Is this the configuration step the consultant needs to complete?

Option	Your Response	Correct Response	Feedback
Add the LinkedIn identity provider (IdP) in Okta with the Account Link policy set to **enabled**.	No	No	This option is incorrect because the Account Link policy is used to specify whether Okta automatically links the user's IdP account with a matching Okta account.
Add the LinkedIn identity provider (IdP) in Okta with the Account Link policy set to **disabled**.	No	No	This option is incorrect because the Account Link policy is used to specify whether Okta automatically links the user's IdP account with a matching Okta account.
Add the LinkedIn identity provider (IdP) in Okta with Auto-Link restrictions set to link the user's IdP account with a matching Okta account.	No	No	This option is incorrect because setting the Auto-Link restrictions to link the user's IdP account with a matching Okta account would not meet the requirement of the scenario that existing Okta accounts who are members of the Okta-LinkedIn group should be auto-linked.
Add the LinkedIn identity provider (IdP) in Okta with Auto-Link restrictions set to the Okta-LinkedIn group.	Yes	Yes	This option is correct because specifying the Okta-LinkedIn group in the Auto-Link restrictions ensures that only existing Okta accounts who are members of the Okta-LinkedIn group are auto-linked.

Score
100%

Feedback



3. Question

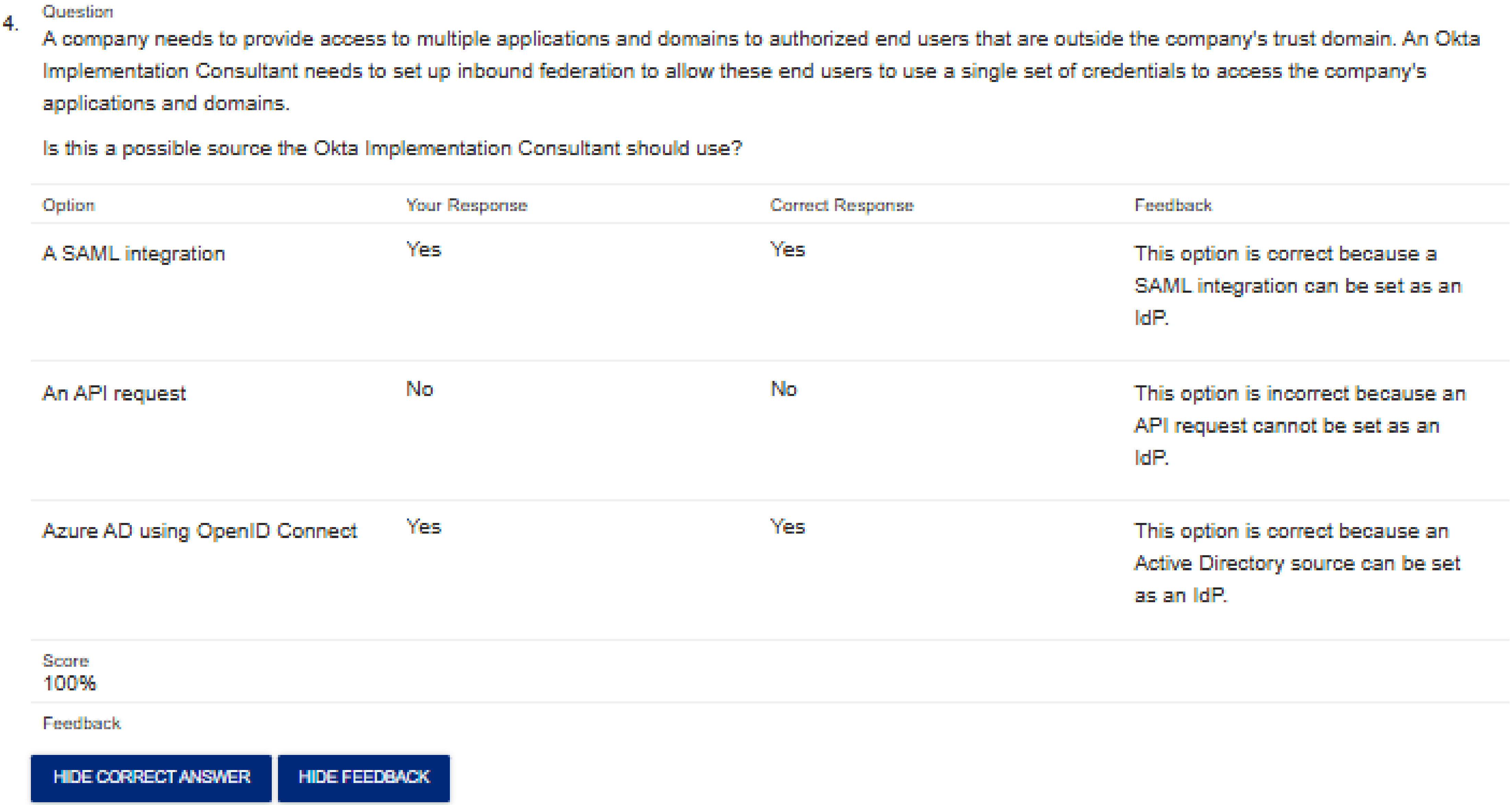
An Okta Implementation Consultant is configuring Okta API Access Management to protect a customer's APIs. An OAuth 2.0 Client is configured in multiple access policies and multiple authorization servers.

Is this an expected behavior for this OAuth 2.0 Client?

Option	Your Response	Correct Response	Feedback
Multiple tokens will be generated, each with separate authorization policies, token expiration times, and scopes.	Yes	Yes	This option is correct because an OAuth 2.0 client can be assigned to any number of authorization servers. Doing so provides for a variety of tokens to be generated, each with separate authorization policies, token expiration times, and scopes.
Unexpected scopes could be generated.	No	No	This option is incorrect because if a request generates unexpected scopes, it is because of an overly broad rule within the authorization server.
The Resource Owner Password grant type will be used to determine which scopes are generated.	No	No	This option is incorrect because Okta recommends not using the resource owner password grant type in this scenario.
Access tokens can be retrieved from the various authorization servers.	Yes	Yes	This option is correct because OAuth clients and authorization servers can be assigned on a many-to-many basis. This allows a developer to use a single OAuth client to retrieve access tokens from different authorization servers depending on the use case.

Score
100%

Feedback



4. Question

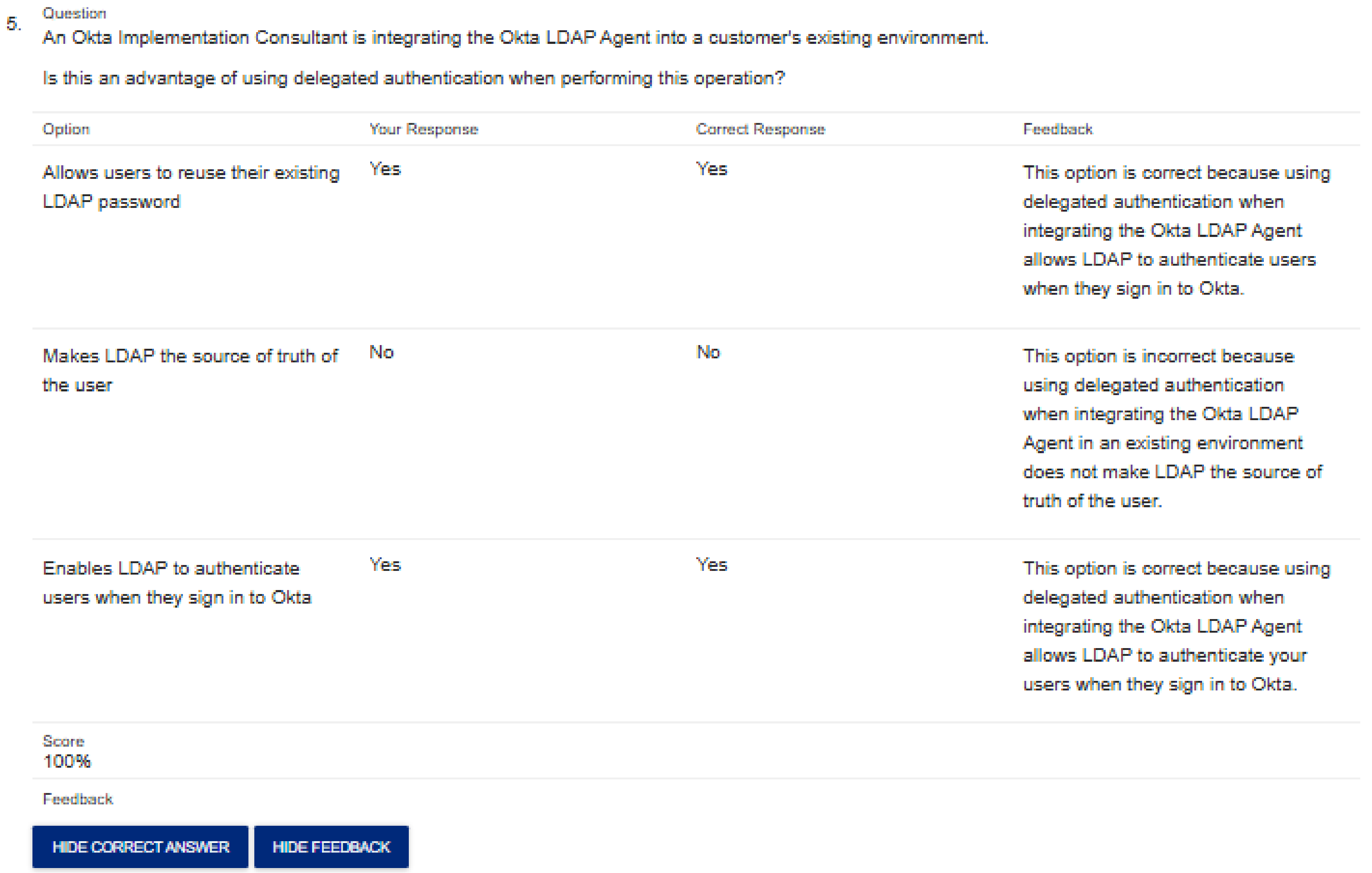
A company needs to provide access to multiple applications and domains to authorized end users that are outside the company's trust domain. An Okta Implementation Consultant needs to set up inbound federation to allow these end users to use a single set of credentials to access the company's applications and domains.

Is this a possible source the Okta Implementation Consultant should use?

Option	Your Response	Correct Response	Feedback
A SAML integration	Yes	Yes	This option is correct because a SAML integration can be set as an IdP.
An API request	No	No	This option is incorrect because an API request cannot be set as an IdP.
Azure AD using OpenID Connect	Yes	Yes	This option is correct because an Active Directory source can be set as an IdP.

Score
100%

Feedback



5. Question

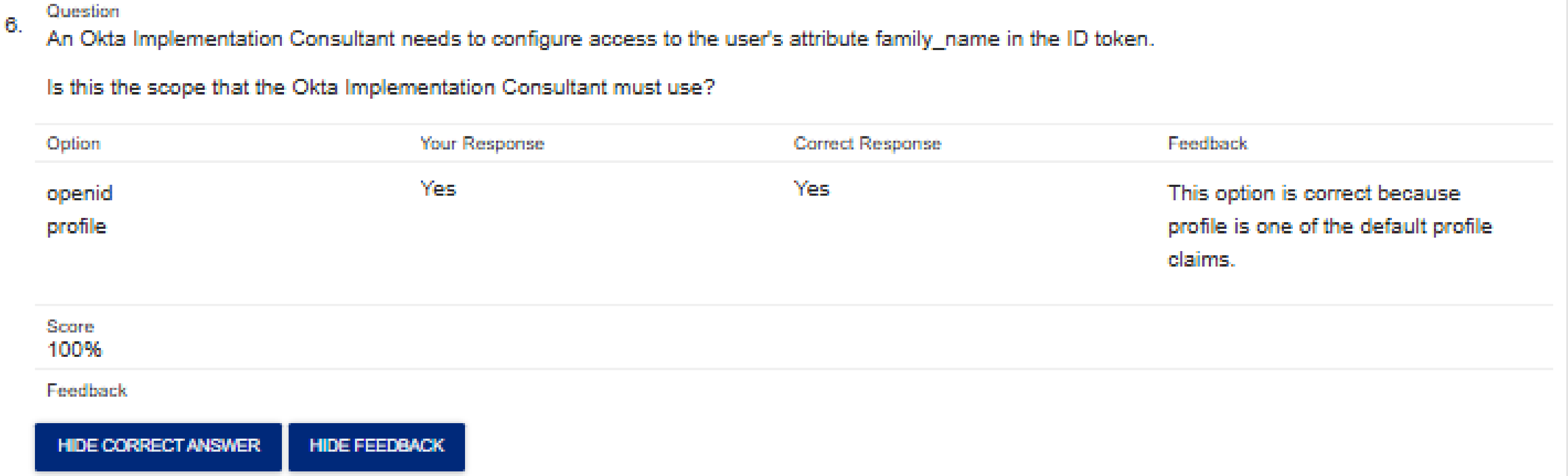
An Okta Implementation Consultant is integrating the Okta LDAP Agent into a customer's existing environment.

Is this an advantage of using delegated authentication when performing this operation?

Option	Your Response	Correct Response	Feedback
Allows users to reuse their existing LDAP password	Yes	Yes	This option is correct because using delegated authentication when integrating the Okta LDAP Agent allows LDAP to authenticate users when they sign in to Okta.
Makes LDAP the source of truth of the user	No	No	This option is incorrect because using delegated authentication when integrating the Okta LDAP Agent in an existing environment does not make LDAP the source of truth of the user.
Enables LDAP to authenticate users when they sign in to Okta	Yes	Yes	This option is correct because using delegated authentication when integrating the Okta LDAP Agent allows LDAP to authenticate your users when they sign in to Okta.

Score
100%

Feedback



6. Question

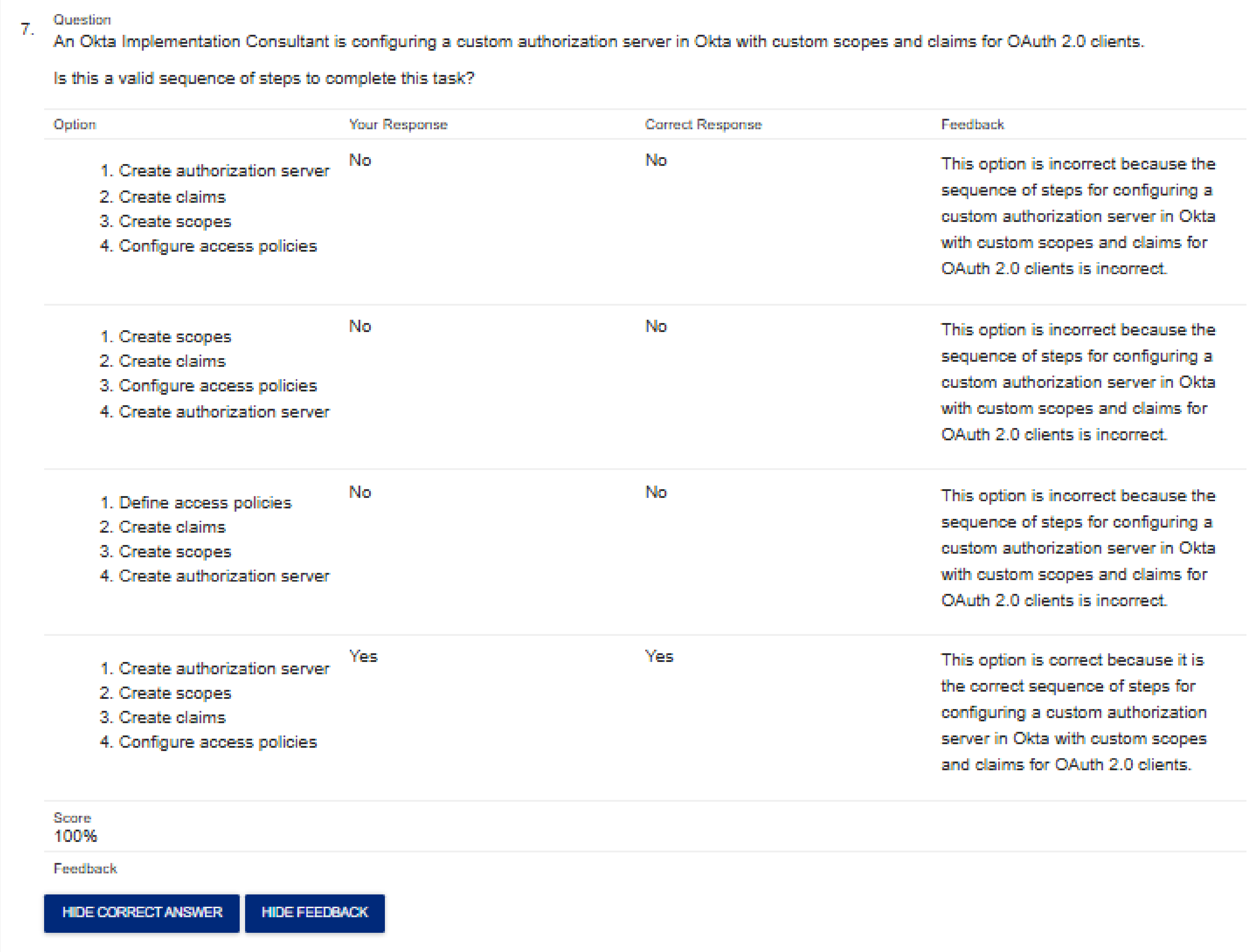
An Okta Implementation Consultant needs to configure access to the user's attribute family_name in the ID token.

Is this the scope that the Okta Implementation Consultant must use?

Option	Your Response	Correct Response	Feedback
openid profile	Yes	Yes	This option is correct because profile is one of the default profile claims.

Score
100%

Feedback



7. Question

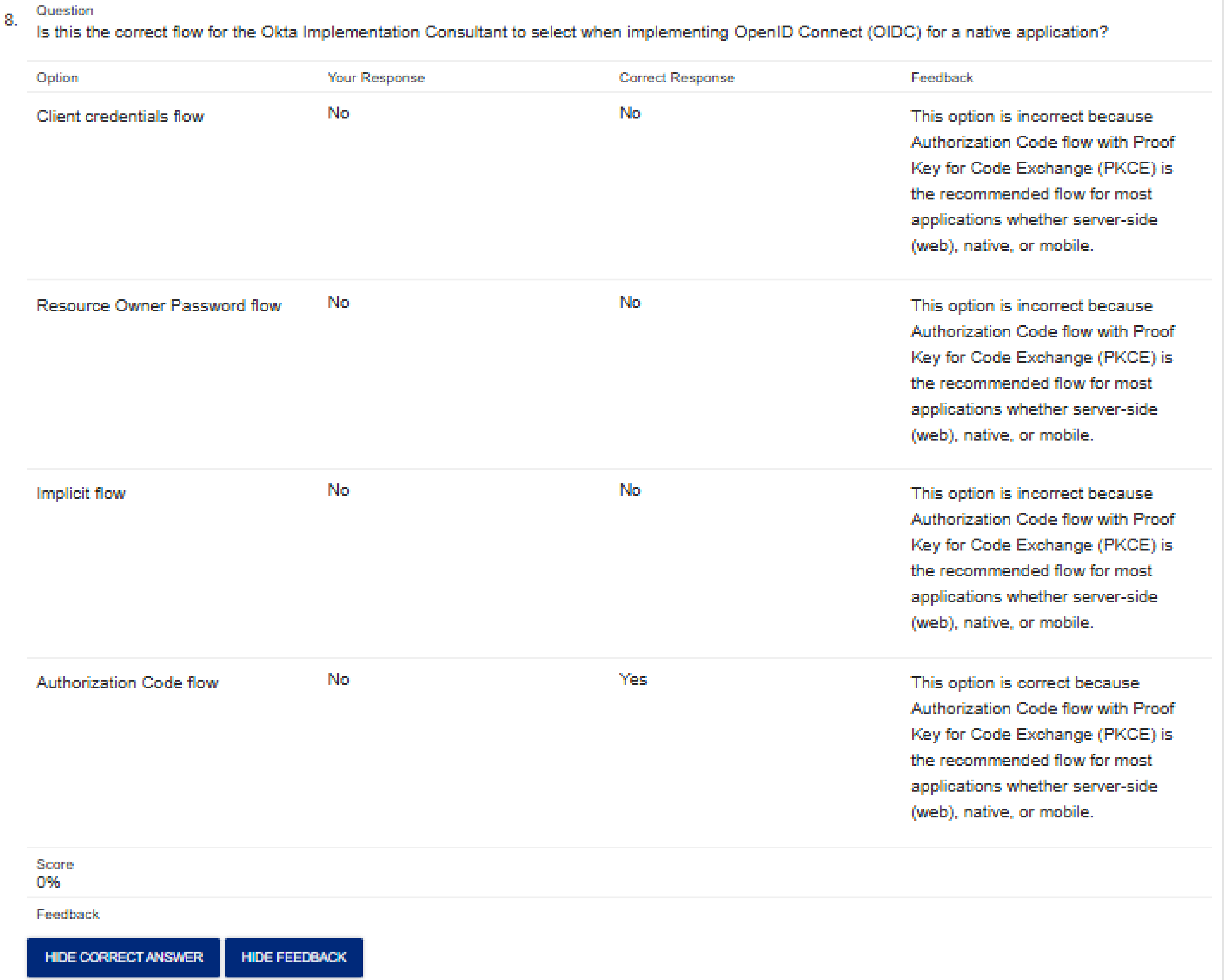
An Okta Implementation Consultant is configuring a custom authorization server in Okta with custom scopes and claims for OAuth 2.0 clients.

Is this a valid sequence of steps to complete this task?

Option	Your Response	Correct Response	Feedback
1. Create authorization server 2. Create claims 3. Create scopes 4. Configure access policies	No	No	This option is incorrect because the sequence of steps for configuring a custom authorization server in Okta with custom scopes and claims for OAuth 2.0 clients is incorrect.
1. Create scopes 2. Create claims 3. Configure access policies 4. Create authorization server	No	No	This option is incorrect because the sequence of steps for configuring a custom authorization server in Okta with custom scopes and claims for OAuth 2.0 clients is incorrect.
1. Define access policies 2. Create claims 3. Create scopes 4. Create authorization server	No	No	This option is incorrect because the sequence of steps for configuring a custom authorization server in Okta with custom scopes and claims for OAuth 2.0 clients is incorrect.
1. Create authorization server 2. Create scopes 3. Create claims 4. Configure access policies	Yes	Yes	This option is correct because it is the correct sequence of steps for configuring a custom authorization server in Okta with custom scopes and claims for OAuth 2.0 clients.

Score
100%

Feedback



8. Question

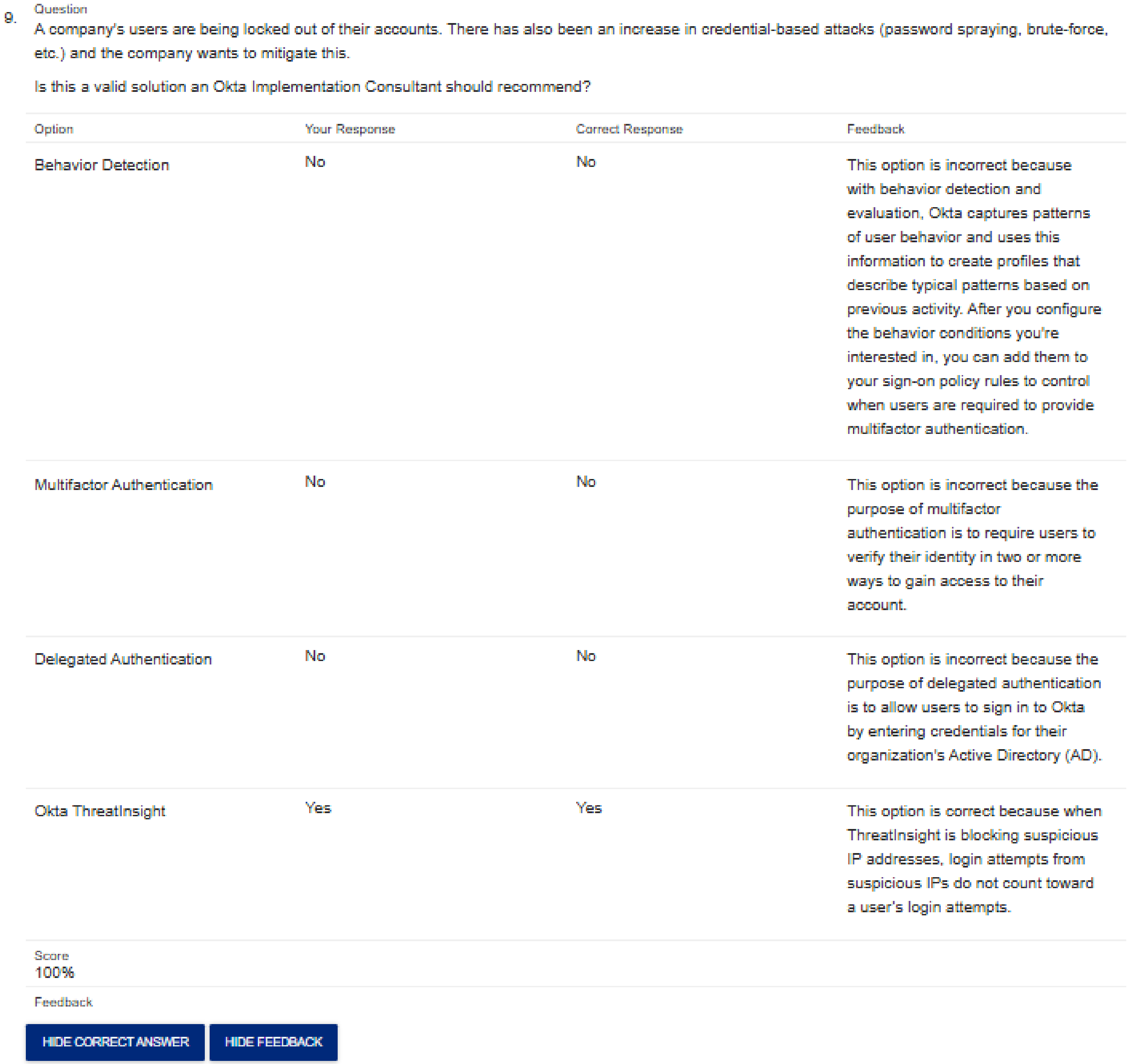
Is this the correct flow for the Okta Implementation Consultant to select when implementing OpenID Connect (OIDC) for a native application?

Option	Your Response	Correct Response	Feedback
Client credentials flow	No	No	This option is incorrect because Authorization Code flow with Proof Key for Code Exchange (PKCE) is the recommended flow for most applications whether server-side (web), native, or mobile.
Resource Owner Password flow	No	No	This option is incorrect because Authorization Code flow with Proof Key for Code Exchange (PKCE) is the recommended flow for most applications whether server-side (web), native, or mobile.
Implicit flow	No	No	This option is incorrect because Authorization Code flow with Proof Key for Code Exchange (PKCE) is the recommended flow for most applications whether server-side (web), native, or mobile.
Authorization Code flow	No	Yes	This option is correct because Authorization Code flow with Proof Key for Code Exchange (PKCE) is the recommended flow for most applications whether server-side (web), native, or mobile.

Score

0%

Feedback



9. Question

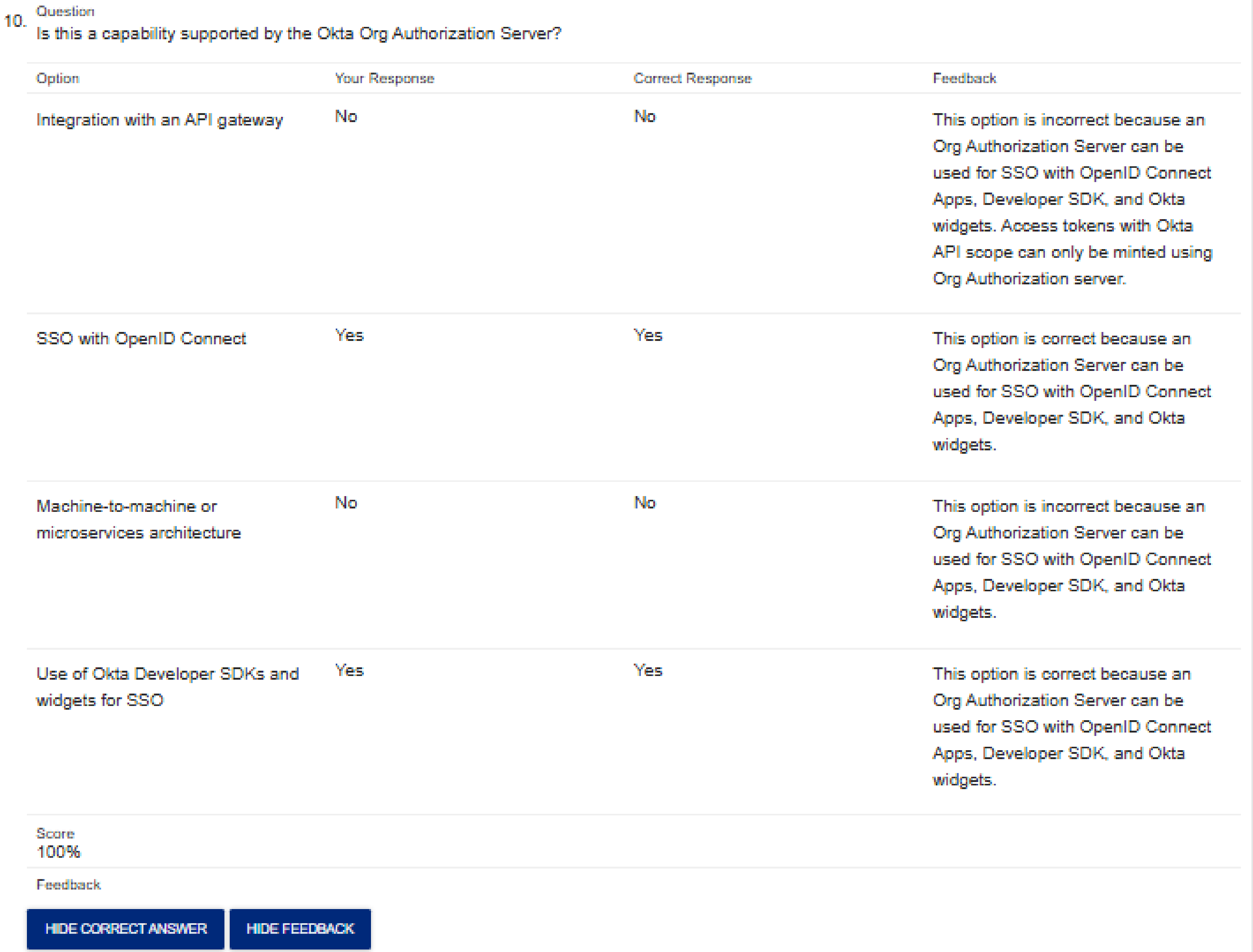
A company's users are being locked out of their accounts. There has also been an increase in credential-based attacks (password spraying, brute-force, etc.) and the company wants to mitigate this.

Is this a valid solution an Okta Implementation Consultant should recommend?

Option	Your Response	Correct Response	Feedback
Behavior Detection	No	No	This option is incorrect because with behavior detection and evaluation, Okta captures patterns of user behavior and uses this information to create profiles that describe typical patterns based on previous activity. After you configure the behavior conditions you're interested in, you can add them to your sign-on policy rules to control when users are required to provide multifactor authentication.
Multifactor Authentication	No	No	This option is incorrect because the purpose of multifactor authentication is to require users to verify their identity in two or more ways to gain access to their account.
Delegated Authentication	No	No	This option is incorrect because the purpose of delegated authentication is to allow users to sign in to Okta by entering credentials for their organization's Active Directory (AD).
Okta ThreatInsight	Yes	Yes	This option is correct because when ThreatInsight is blocking suspicious IP addresses, login attempts from suspicious IPs do not count toward a user's login attempts.

Score
100%

Feedback



10. Question

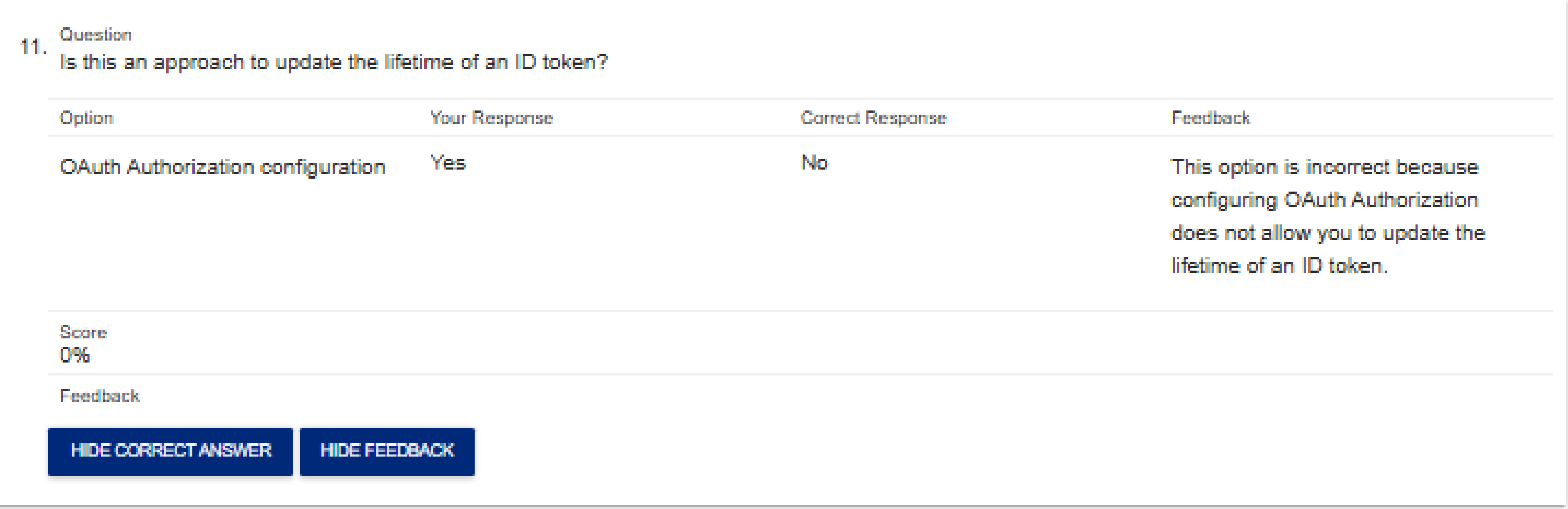
Is this a capability supported by the Okta Org Authorization Server?

Option	Your Response	Correct Response	Feedback
Integration with an API gateway	No	No	This option is incorrect because an Org Authorization Server can be used for SSO with OpenID Connect Apps, Developer SDK, and Okta widgets. Access tokens with Okta API scope can only be minted using Org Authorization server.
SSO with OpenID Connect	Yes	Yes	This option is correct because an Org Authorization Server can be used for SSO with OpenID Connect Apps, Developer SDK, and Okta widgets.
Machine-to-machine or microservices architecture	No	No	This option is incorrect because an Org Authorization Server can be used for SSO with OpenID Connect Apps, Developer SDK, and Okta widgets.
Use of Okta Developer SDKs and widgets for SSO	Yes	Yes	This option is correct because an Org Authorization Server can be used for SSO with OpenID Connect Apps, Developer SDK, and Okta widgets.

Score

100%

Feedback



11. Question

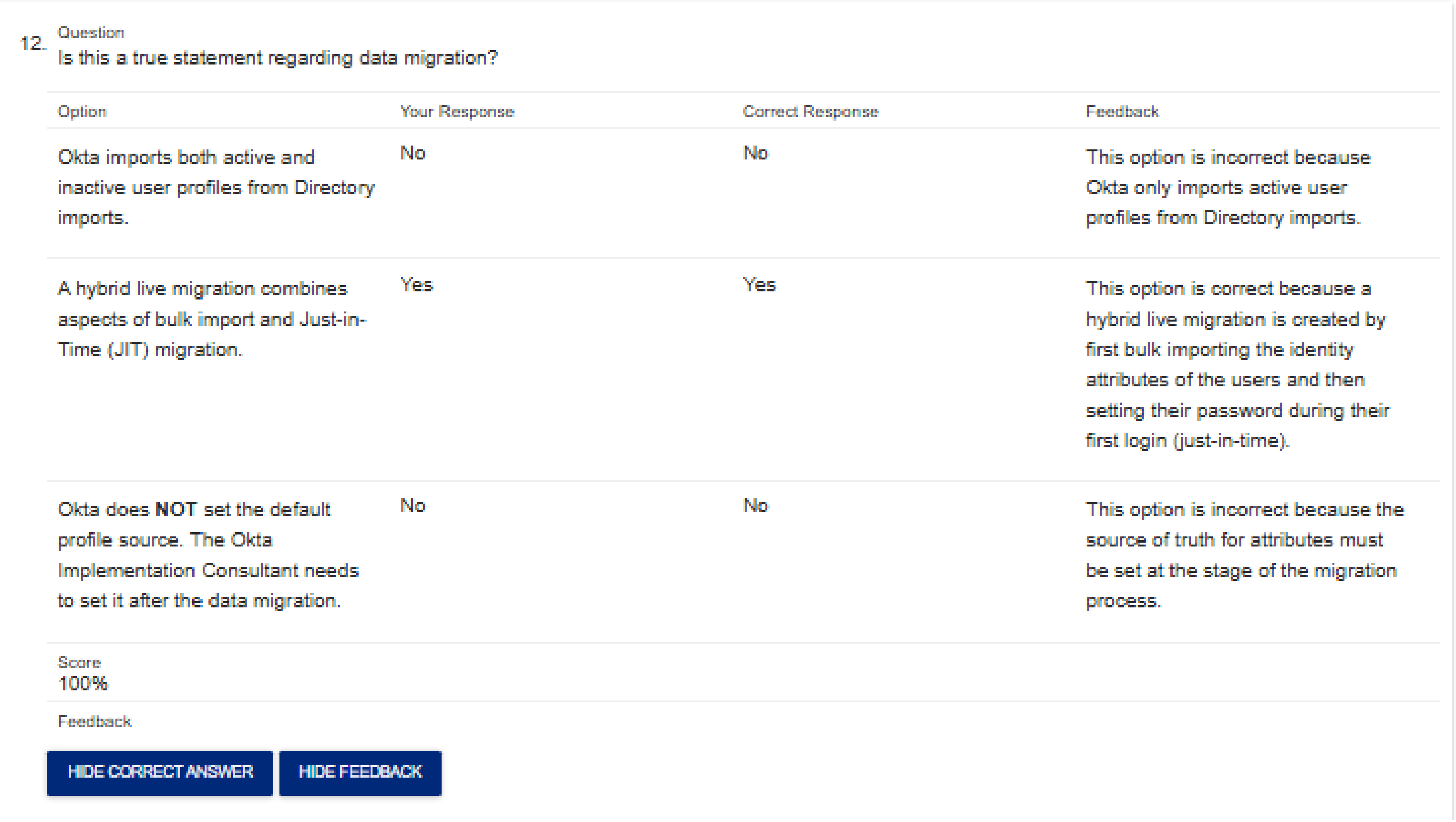
Is this an approach to update the lifetime of an ID token?

Option	Your Response	Correct Response	Feedback
OAuth Authorization configuration	Yes	No	This option is incorrect because configuring OAuth Authorization does not allow you to update the lifetime of an ID token.

Score

0%

Feedback



12. Question

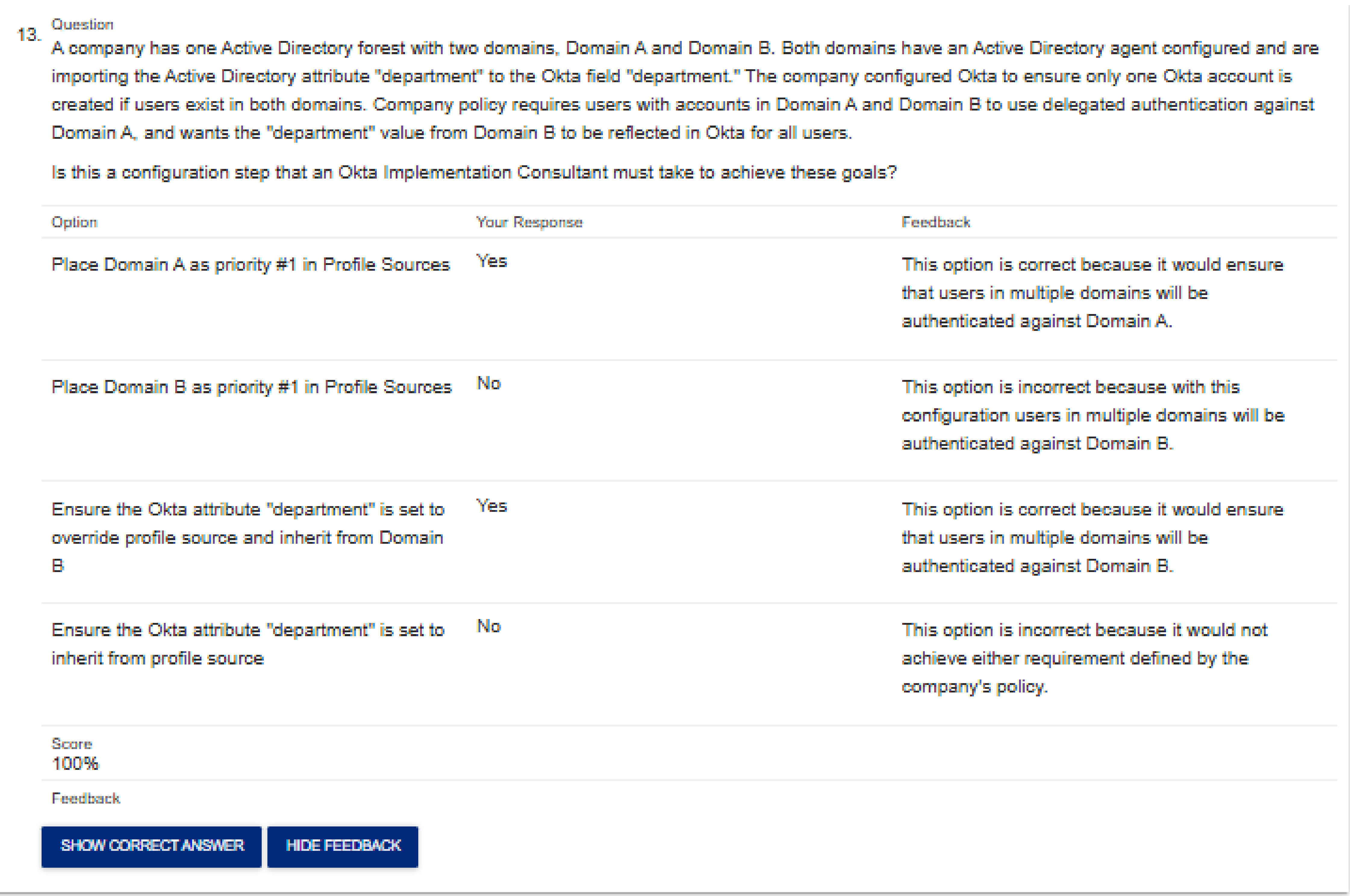
Is this a true statement regarding data migration?

Option	Your Response	Correct Response	Feedback
Okta imports both active and inactive user profiles from Directory imports.	No	No	This option is incorrect because Okta only imports active user profiles from Directory imports.
A hybrid live migration combines aspects of bulk import and Just-in-Time (JIT) migration.	Yes	Yes	This option is correct because a hybrid live migration is created by first bulk importing the identity attributes of the users and then setting their password during their first login (just-in-time).
Okta does **NOT** set the default profile source. The Okta Implementation Consultant needs to set it after the data migration.	No	No	This option is incorrect because the source of truth for attributes must be set at the stage of the migration process.

Score

100%

Feedback



13. Question

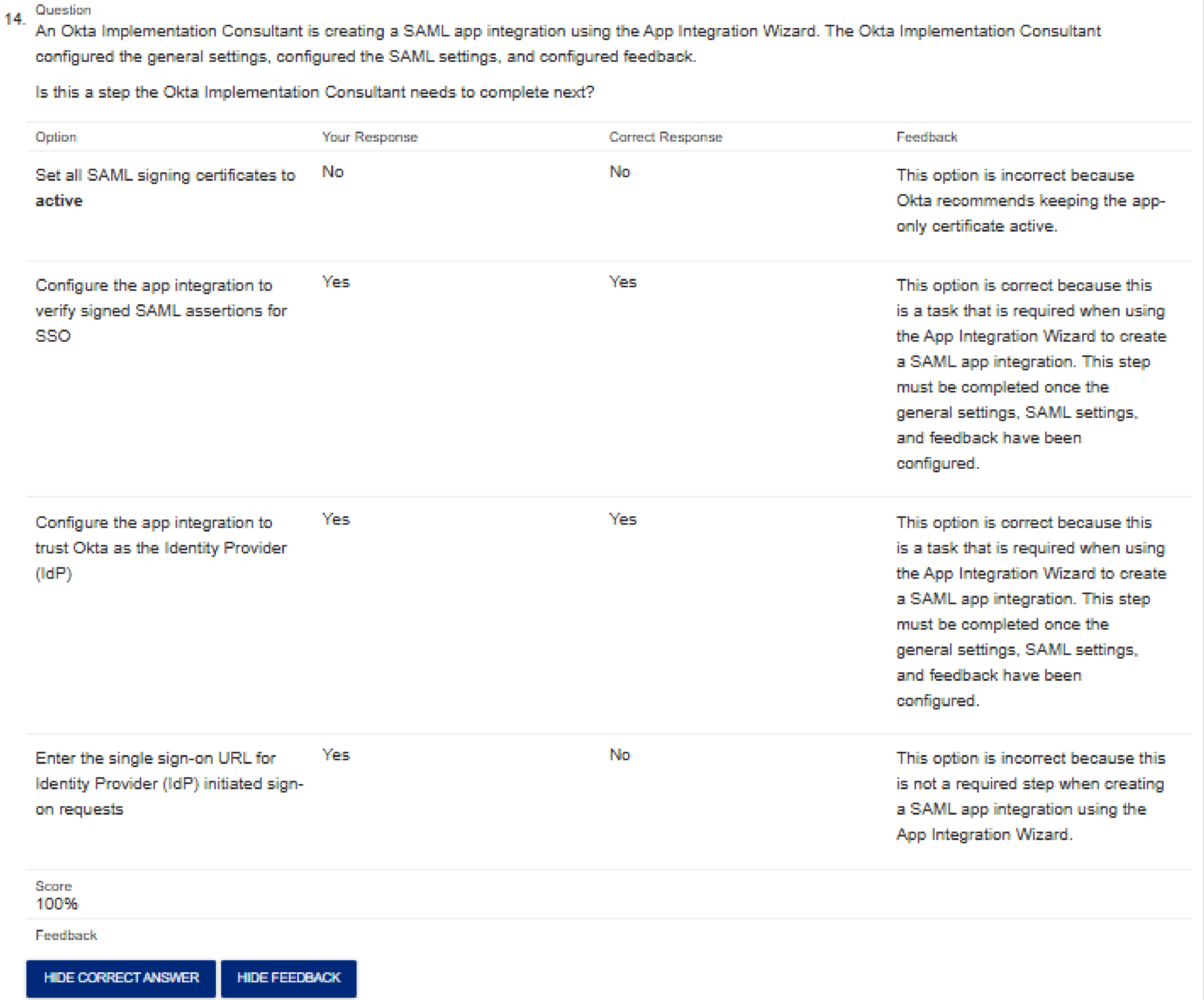
A company has one Active Directory forest with two domains, Domain A and Domain B. Both domains have an Active Directory agent configured and are importing the Active Directory attribute "department" to the Okta field "department." The company configured Okta to ensure only one Okta account is created if users exist in both domains. Company policy requires users with accounts in Domain A and Domain B to use delegated authentication against Domain A, and wants the "department" value from Domain B to be reflected in Okta for all users.

Is this a configuration step that an Okta Implementation Consultant must take to achieve these goals?

Option	Your Response	Feedback
Place Domain A as priority #1 in Profile Sources	Yes	This option is correct because it would ensure that users in multiple domains will be authenticated against Domain A.
Place Domain B as priority #1 in Profile Sources	No	This option is incorrect because with this configuration users in multiple domains will be authenticated against Domain B.
Ensure the Okta attribute "department" is set to override profile source and inherit from Domain B	Yes	This option is correct because it would ensure that users in multiple domains will be authenticated against Domain B.
Ensure the Okta attribute "department" is set to inherit from profile source	No	This option is incorrect because it would not achieve either requirement defined by the company's policy.

Score
100%

Feedback



14. Question

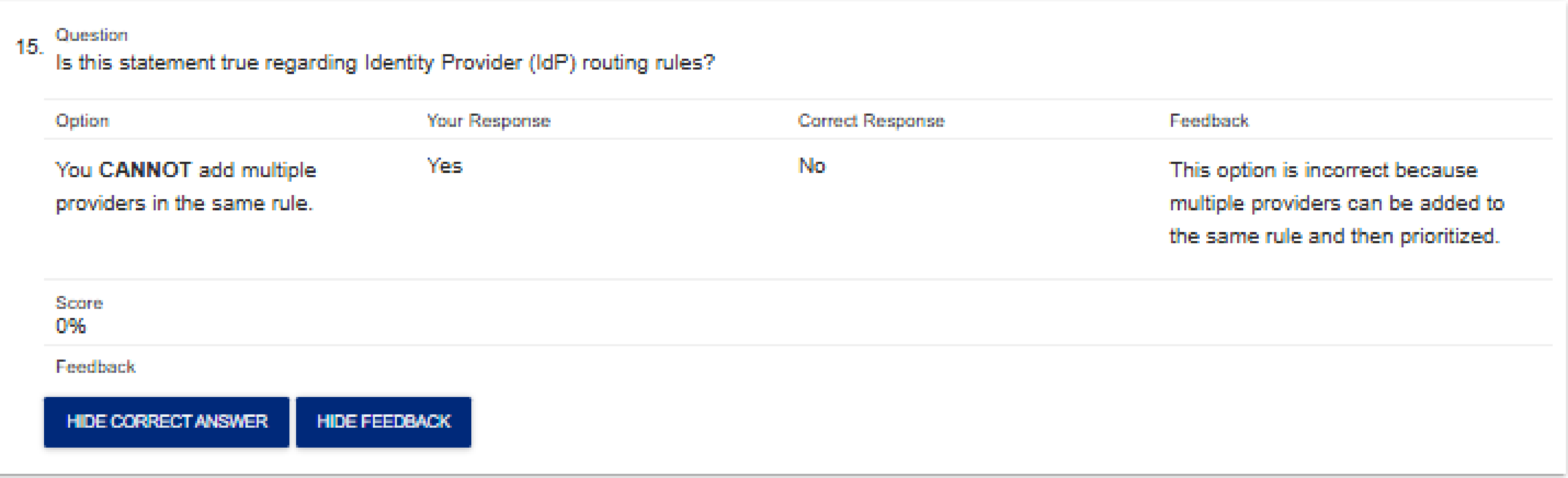
An Okta Implementation Consultant is creating a SAML app integration using the App Integration Wizard. The Okta Implementation Consultant configured the general settings, configured the SAML settings, and configured feedback.

Is this a step the Okta Implementation Consultant needs to complete next?

Option	Your Response	Correct Response	Feedback
Set all SAML signing certificates to **active**	No	No	This option is incorrect because Okta recommends keeping the app-only certificate active.
Configure the app integration to verify signed SAML assertions for SSO	Yes	Yes	This option is correct because this is a task that is required when using the App Integration Wizard to create a SAML app integration. This step must be completed once the general settings, SAML settings, and feedback have been configured.
Configure the app integration to trust Okta as the Identity Provider (IdP)	Yes	Yes	This option is correct because this is a task that is required when using the App Integration Wizard to create a SAML app integration. This step must be completed once the general settings, SAML settings, and feedback have been configured.
Enter the single sign-on URL for Identity Provider (IdP) initiated sign-on requests	Yes	No	This option is incorrect because this is not a required step when creating a SAML app integration using the App Integration Wizard.

Score
100%

Feedback



15. Question

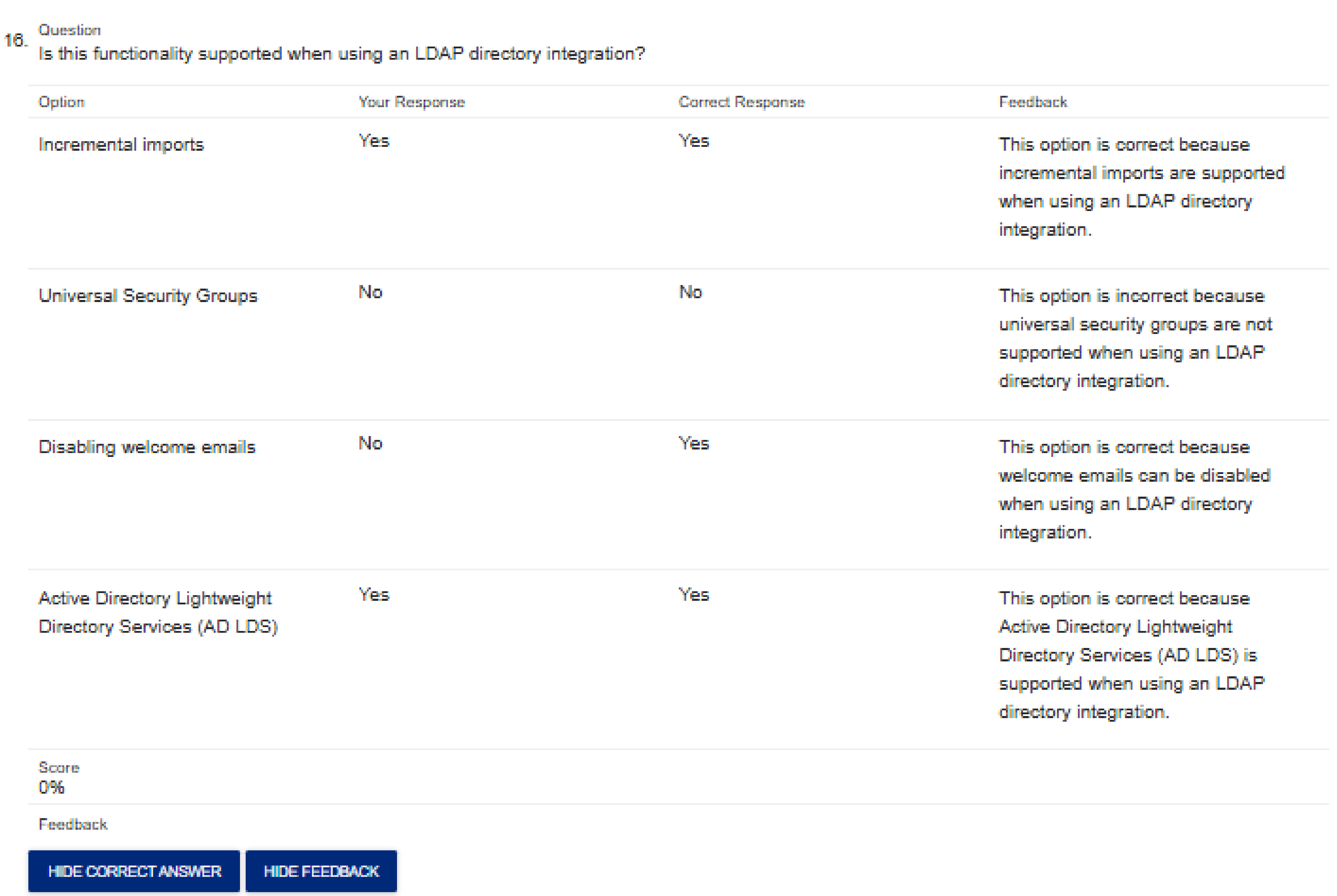
Is this statement true regarding Identity Provider (IdP) routing rules?

Option	Your Response	Correct Response	Feedback
You **CANNOT** add multiple providers in the same rule.	Yes	No	This option is incorrect because multiple providers can be added to the same rule and then prioritized.

Score

0%

Feedback



16. Question

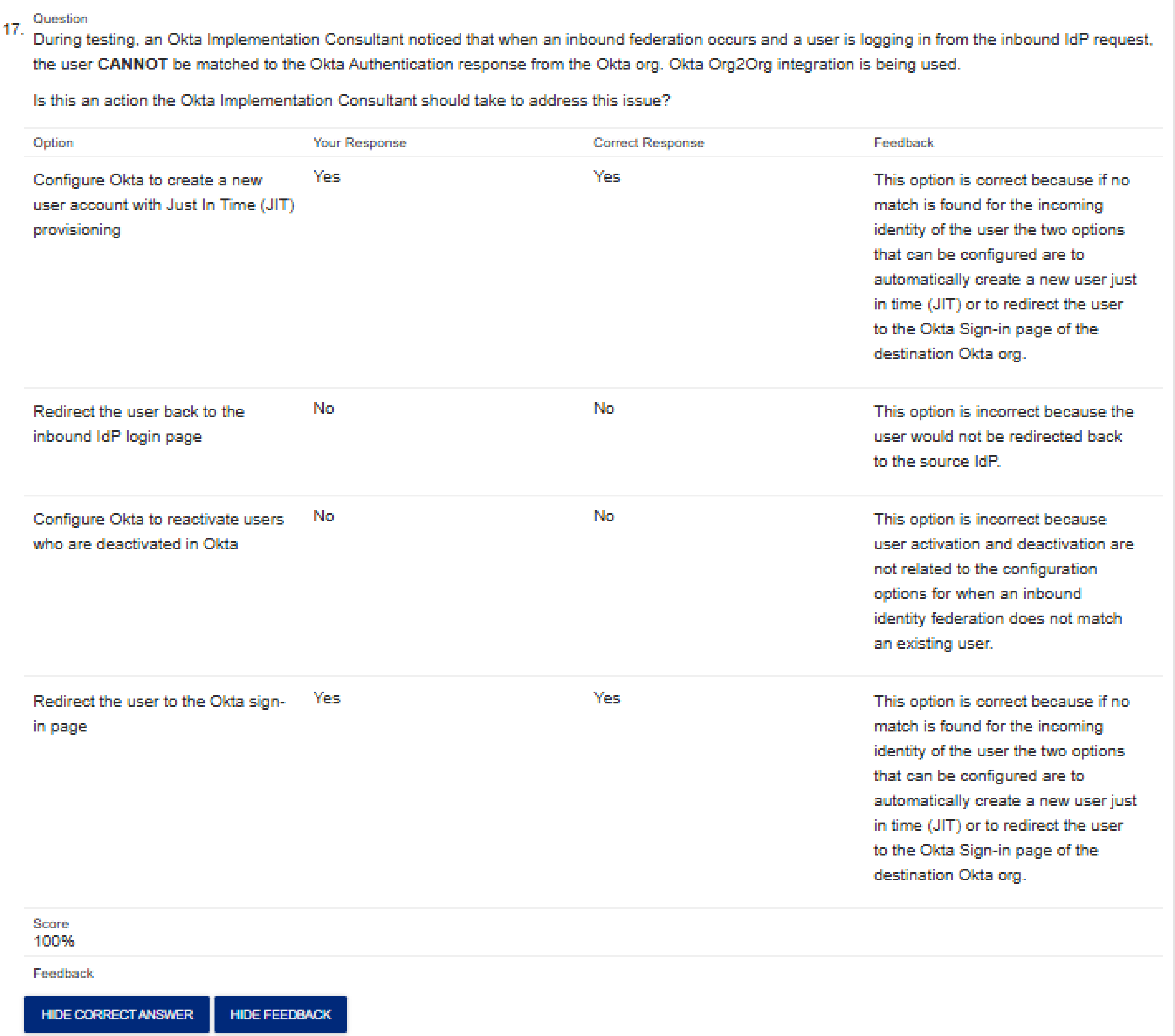
Is this functionality supported when using an LDAP directory integration?

Option	Your Response	Correct Response	Feedback
Incremental imports	Yes	Yes	This option is correct because incremental imports are supported when using an LDAP directory integration.
Universal Security Groups	No	No	This option is incorrect because universal security groups are not supported when using an LDAP directory integration.
Disabling welcome emails	No	Yes	This option is correct because welcome emails can be disabled when using an LDAP directory integration.
Active Directory Lightweight Directory Services (AD LDS)	Yes	Yes	This option is correct because Active Directory Lightweight Directory Services (AD LDS) is supported when using an LDAP directory integration.

Score

0%

Feedback



Question

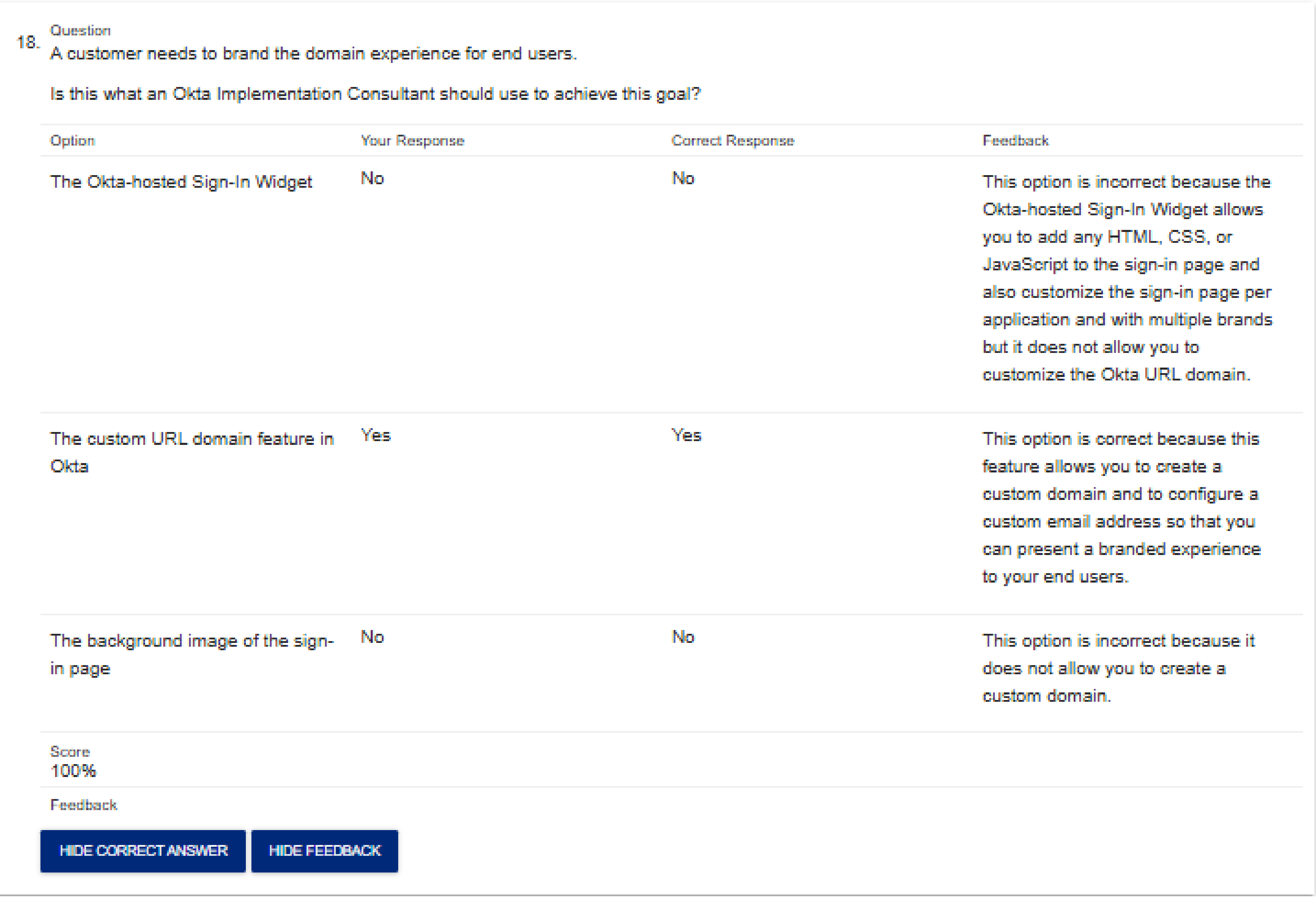
17. During testing, an Okta Implementation Consultant noticed that when an inbound federation occurs and a user is logging in from the inbound IdP request, the user **CANNOT** be matched to the Okta Authentication response from the Okta org. Okta Org2Org integration is being used.

Is this an action the Okta Implementation Consultant should take to address this issue?

Option	Your Response	Correct Response	Feedback
Configure Okta to create a new user account with Just In Time (JIT) provisioning	Yes	Yes	This option is correct because if no match is found for the incoming identity of the user the two options that can be configured are to automatically create a new user just in time (JIT) or to redirect the user to the Okta Sign-in page of the destination Okta org.
Redirect the user back to the inbound IdP login page	No	No	This option is incorrect because the user would not be redirected back to the source IdP.
Configure Okta to reactivate users who are deactivated in Okta	No	No	This option is incorrect because user activation and deactivation are not related to the configuration options for when an inbound identity federation does not match an existing user.
Redirect the user to the Okta sign-in page	Yes	Yes	This option is correct because if no match is found for the incoming identity of the user the two options that can be configured are to automatically create a new user just in time (JIT) or to redirect the user to the Okta Sign-in page of the destination Okta org.

Score
100%

Feedback



18. Question

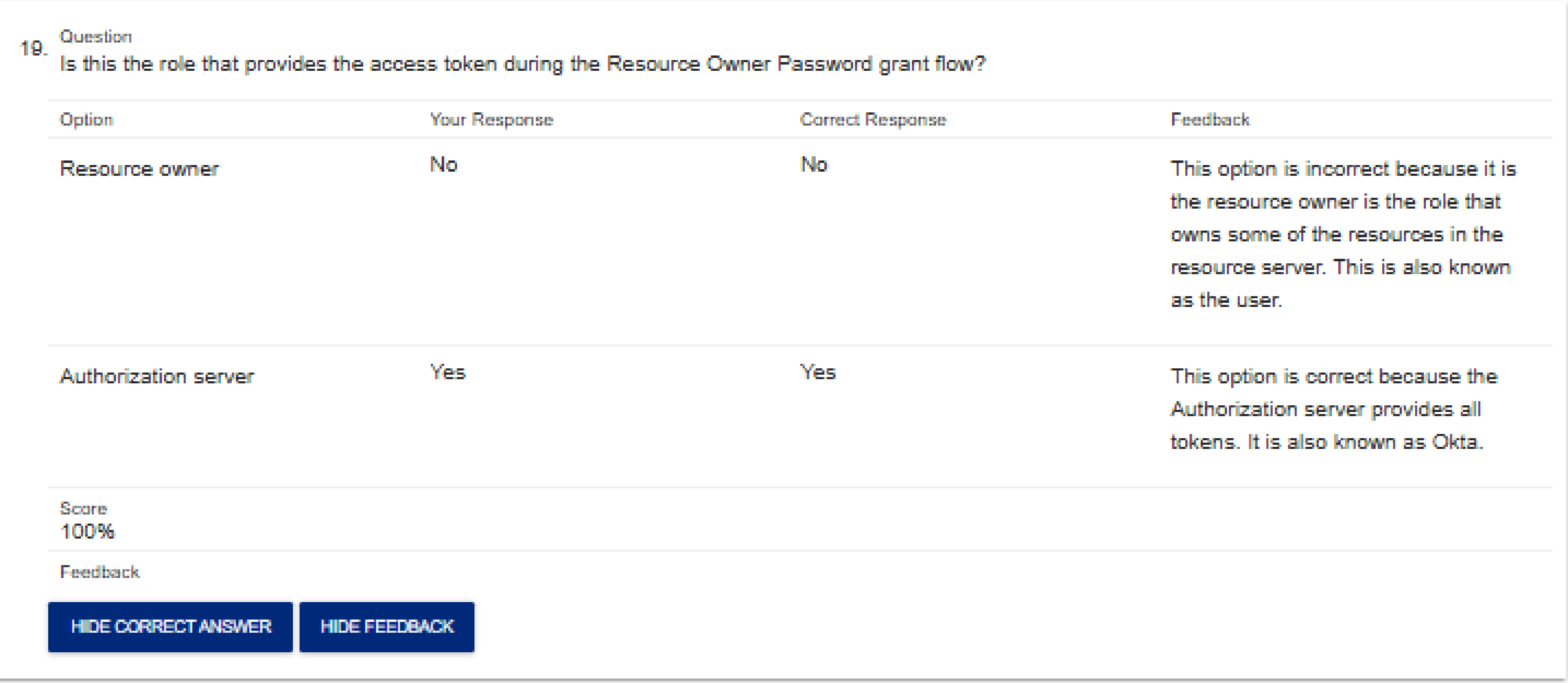
A customer needs to brand the domain experience for end users.

Is this what an Okta Implementation Consultant should use to achieve this goal?

Option	Your Response	Correct Response	Feedback
The Okta-hosted Sign-In Widget	No	No	This option is incorrect because the Okta-hosted Sign-In Widget allows you to add any HTML, CSS, or JavaScript to the sign-in page and also customize the sign-in page per application and with multiple brands but it does not allow you to customize the Okta URL domain.
The custom URL domain feature in Okta	Yes	Yes	This option is correct because this feature allows you to create a custom domain and to configure a custom email address so that you can present a branded experience to your end users.
The background image of the sign-in page	No	No	This option is incorrect because it does not allow you to create a custom domain.

Score
100%

Feedback



19. Question

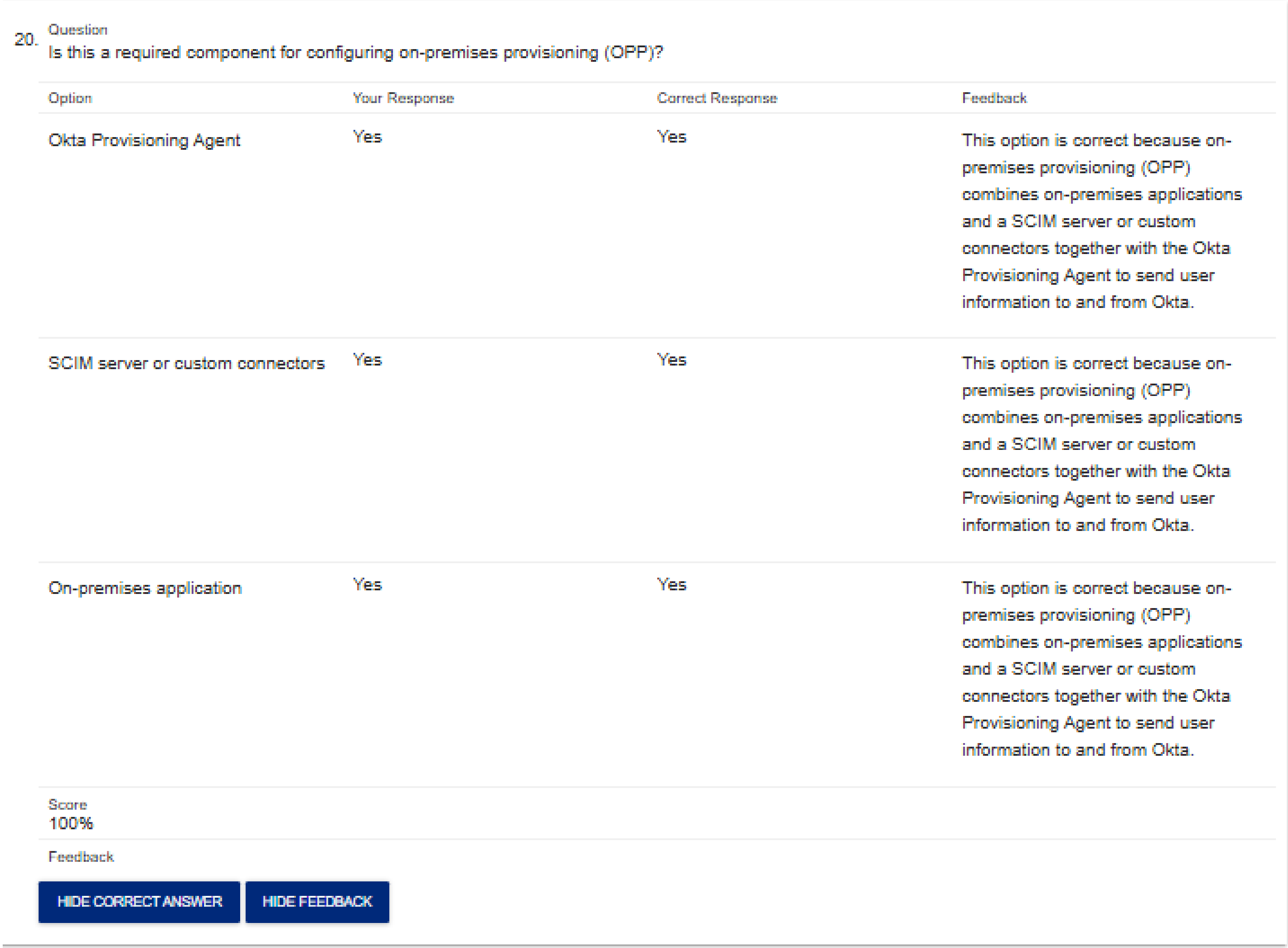
Is this the role that provides the access token during the Resource Owner Password grant flow?

Option	Your Response	Correct Response	Feedback
Resource owner	No	No	This option is incorrect because it is the resource owner is the role that owns some of the resources in the resource server. This is also known as the user.
Authorization server	Yes	Yes	This option is correct because the Authorization server provides all tokens. It is also known as Okta.

Score

100%

Feedback



20. Question

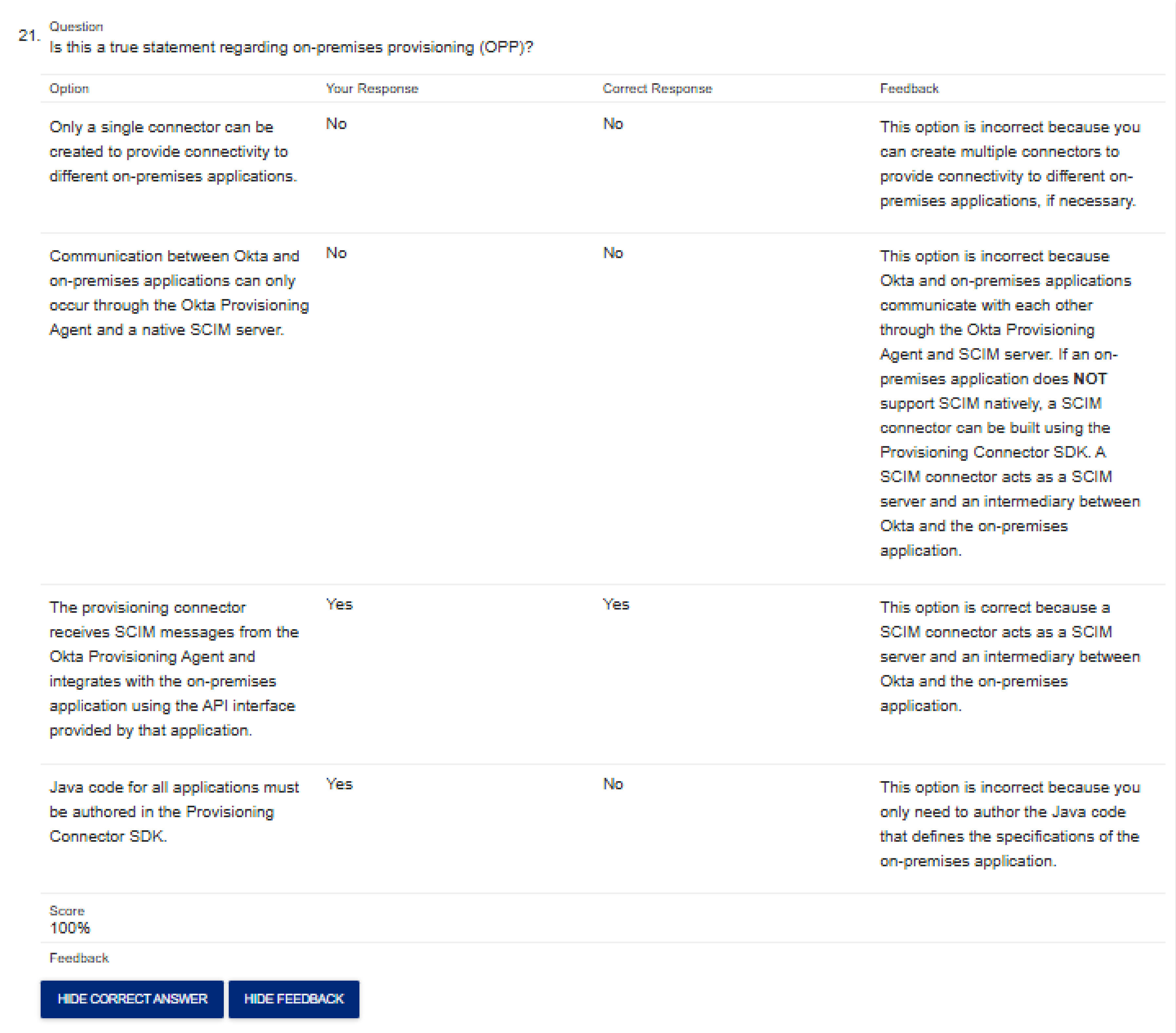
Is this a required component for configuring on-premises provisioning (OPP)?

Option	Your Response	Correct Response	Feedback
Okta Provisioning Agent	Yes	Yes	This option is correct because on-premises provisioning (OPP) combines on-premises applications and a SCIM server or custom connectors together with the Okta Provisioning Agent to send user information to and from Okta.
SCIM server or custom connectors	Yes	Yes	This option is correct because on-premises provisioning (OPP) combines on-premises applications and a SCIM server or custom connectors together with the Okta Provisioning Agent to send user information to and from Okta.
On-premises application	Yes	Yes	This option is correct because on-premises provisioning (OPP) combines on-premises applications and a SCIM server or custom connectors together with the Okta Provisioning Agent to send user information to and from Okta.

Score

100%

Feedback



21. Question

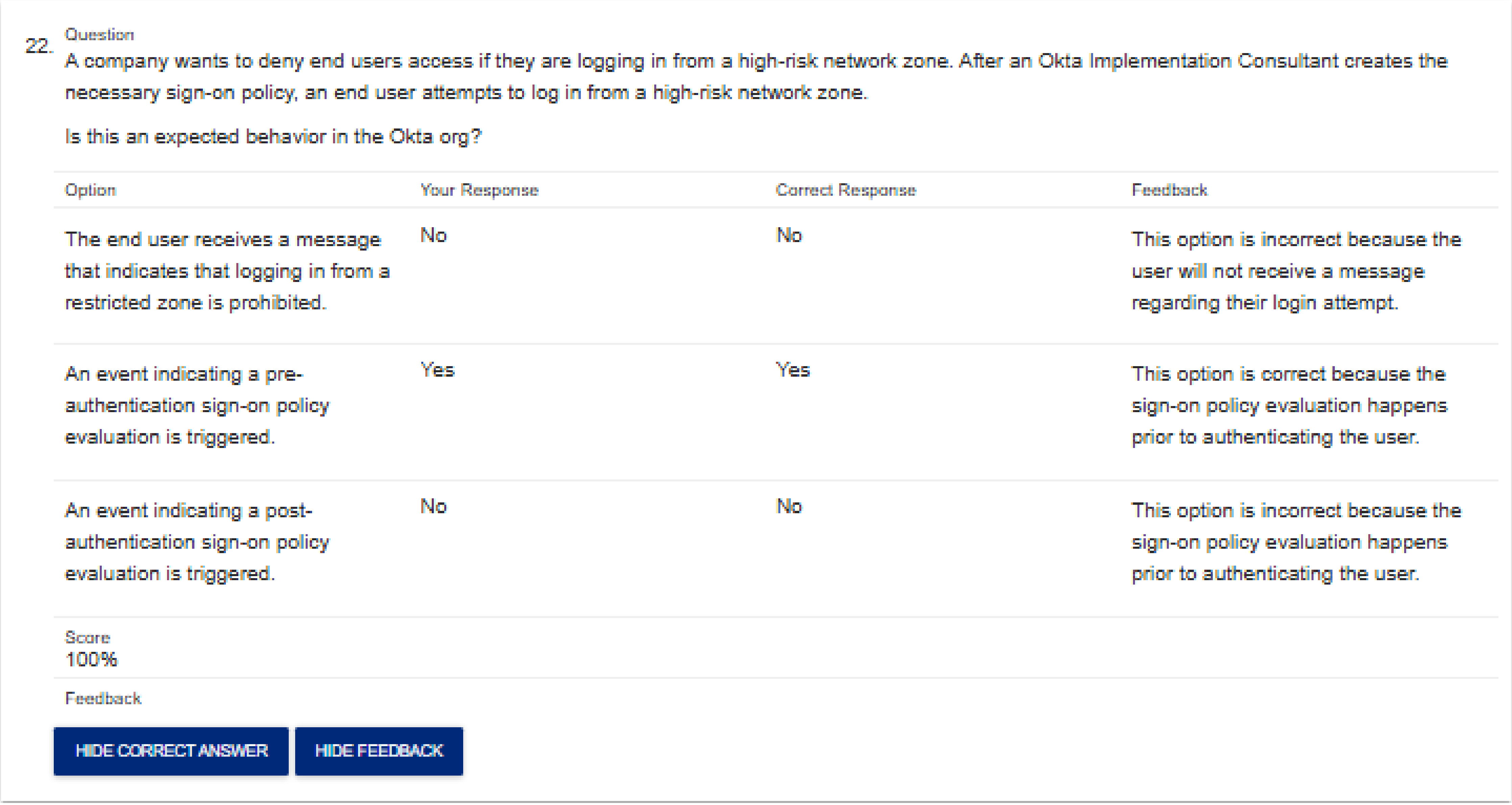
Is this a true statement regarding on-premises provisioning (OPP)?

Option	Your Response	Correct Response	Feedback
Only a single connector can be created to provide connectivity to different on-premises applications.	No	No	This option is incorrect because you can create multiple connectors to provide connectivity to different on-premises applications, if necessary.
Communication between Okta and on-premises applications can only occur through the Okta Provisioning Agent and a native SCIM server.	No	No	This option is incorrect because Okta and on-premises applications communicate with each other through the Okta Provisioning Agent and SCIM server. If an on-premises application does **NOT** support SCIM natively, a SCIM connector can be built using the Provisioning Connector SDK. A SCIM connector acts as a SCIM server and an intermediary between Okta and the on-premises application.
The provisioning connector receives SCIM messages from the Okta Provisioning Agent and integrates with the on-premises application using the API interface provided by that application.	Yes	Yes	This option is correct because a SCIM connector acts as a SCIM server and an intermediary between Okta and the on-premises application.
Java code for all applications must be authored in the Provisioning Connector SDK.	Yes	No	This option is incorrect because you only need to author the Java code that defines the specifications of the on-premises application.

Score

100%

Feedback



22. Question

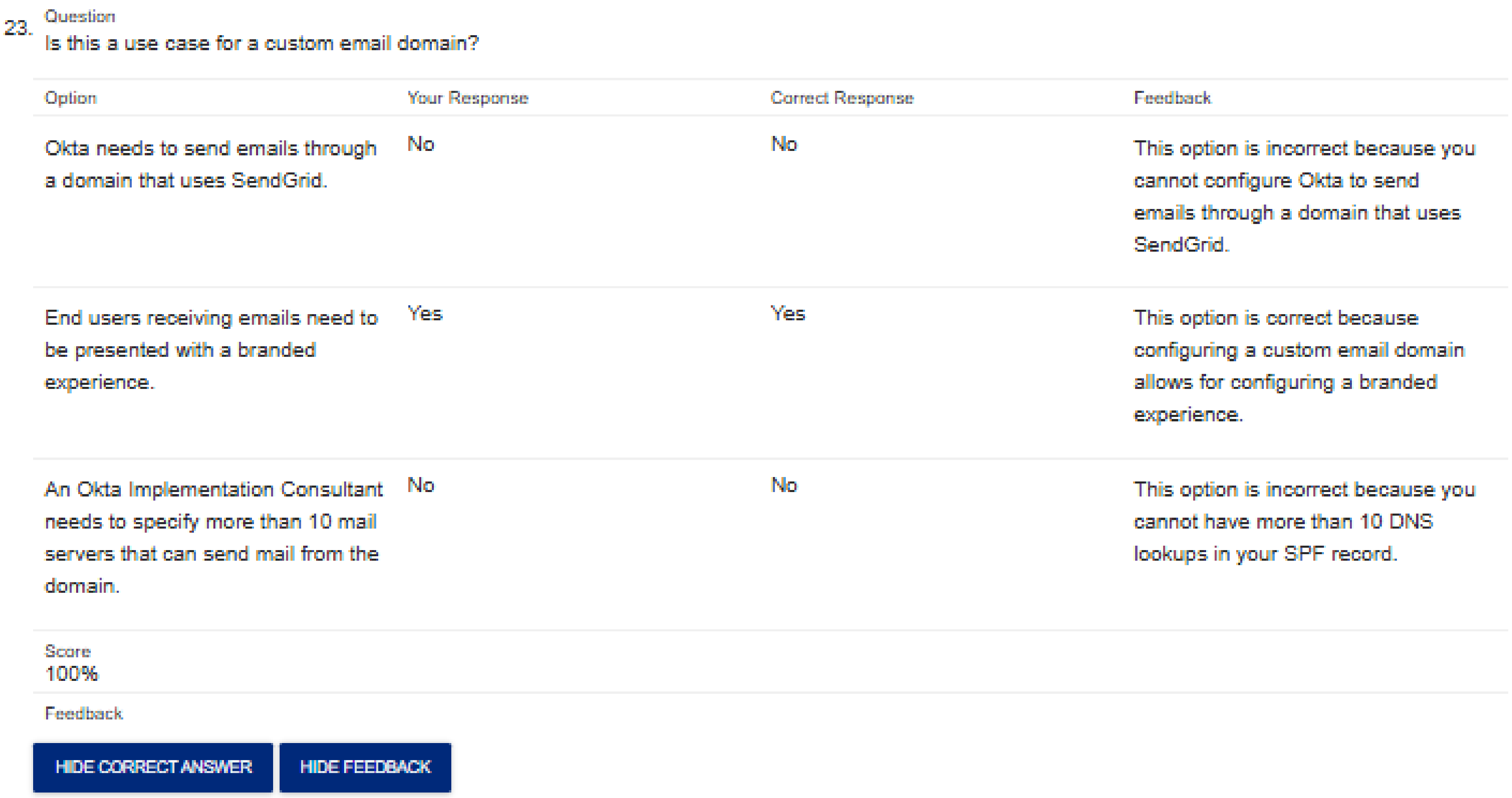
A company wants to deny end users access if they are logging in from a high-risk network zone. After an Okta Implementation Consultant creates the necessary sign-on policy, an end user attempts to log in from a high-risk network zone.

Is this an expected behavior in the Okta org?

Option	Your Response	Correct Response	Feedback
The end user receives a message that indicates that logging in from a restricted zone is prohibited.	No	No	This option is incorrect because the user will not receive a message regarding their login attempt.
An event indicating a pre-authentication sign-on policy evaluation is triggered.	Yes	Yes	This option is correct because the sign-on policy evaluation happens prior to authenticating the user.
An event indicating a post-authentication sign-on policy evaluation is triggered.	No	No	This option is incorrect because the sign-on policy evaluation happens prior to authenticating the user.

Score
100%

Feedback



23. Question

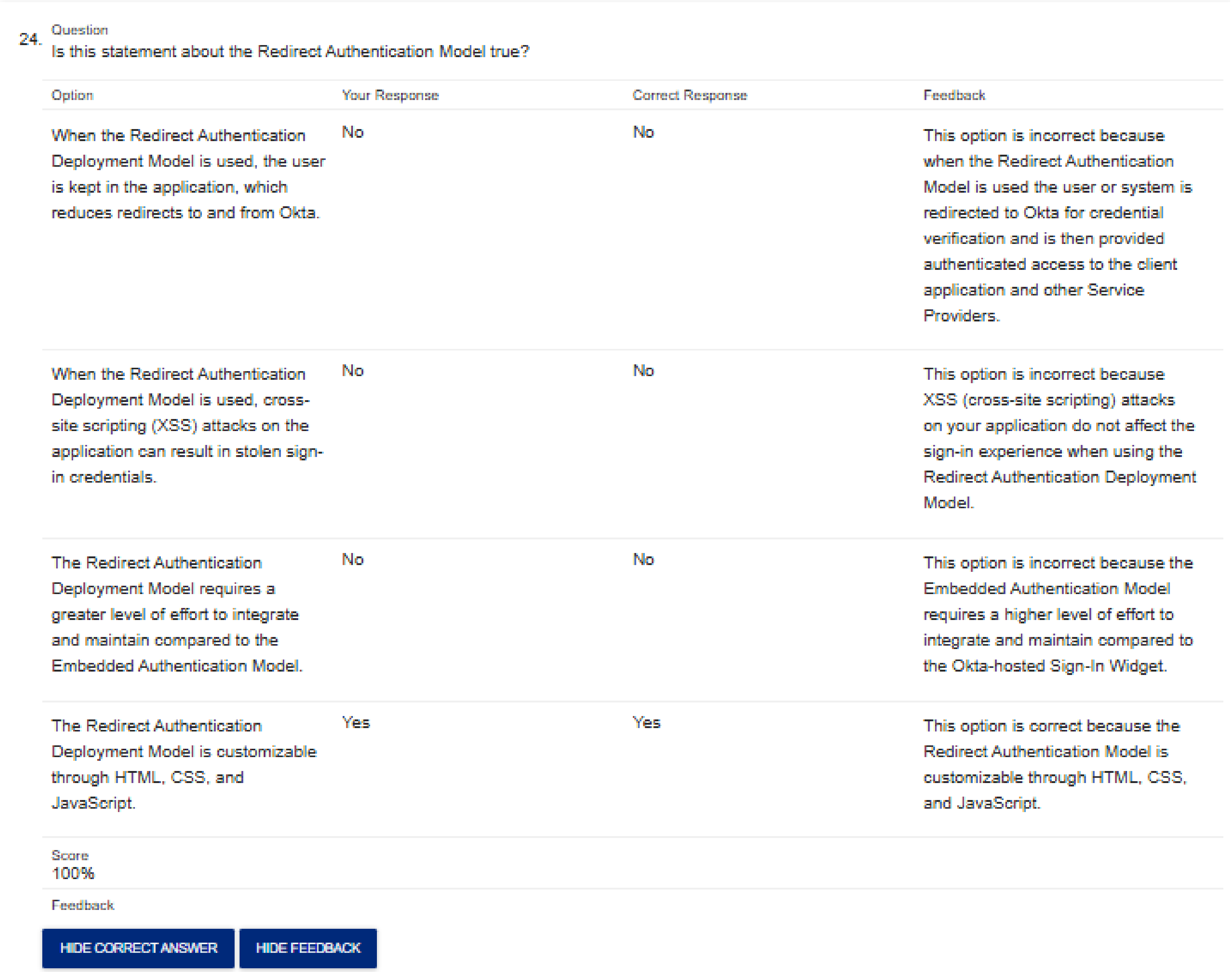
Is this a use case for a custom email domain?

Option	Your Response	Correct Response	Feedback
Okta needs to send emails through a domain that uses SendGrid.	No	No	This option is incorrect because you cannot configure Okta to send emails through a domain that uses SendGrid.
End users receiving emails need to be presented with a branded experience.	Yes	Yes	This option is correct because configuring a custom email domain allows for configuring a branded experience.
An Okta Implementation Consultant needs to specify more than 10 mail servers that can send mail from the domain.	No	No	This option is incorrect because you cannot have more than 10 DNS lookups in your SPF record.

Score

100%

Feedback



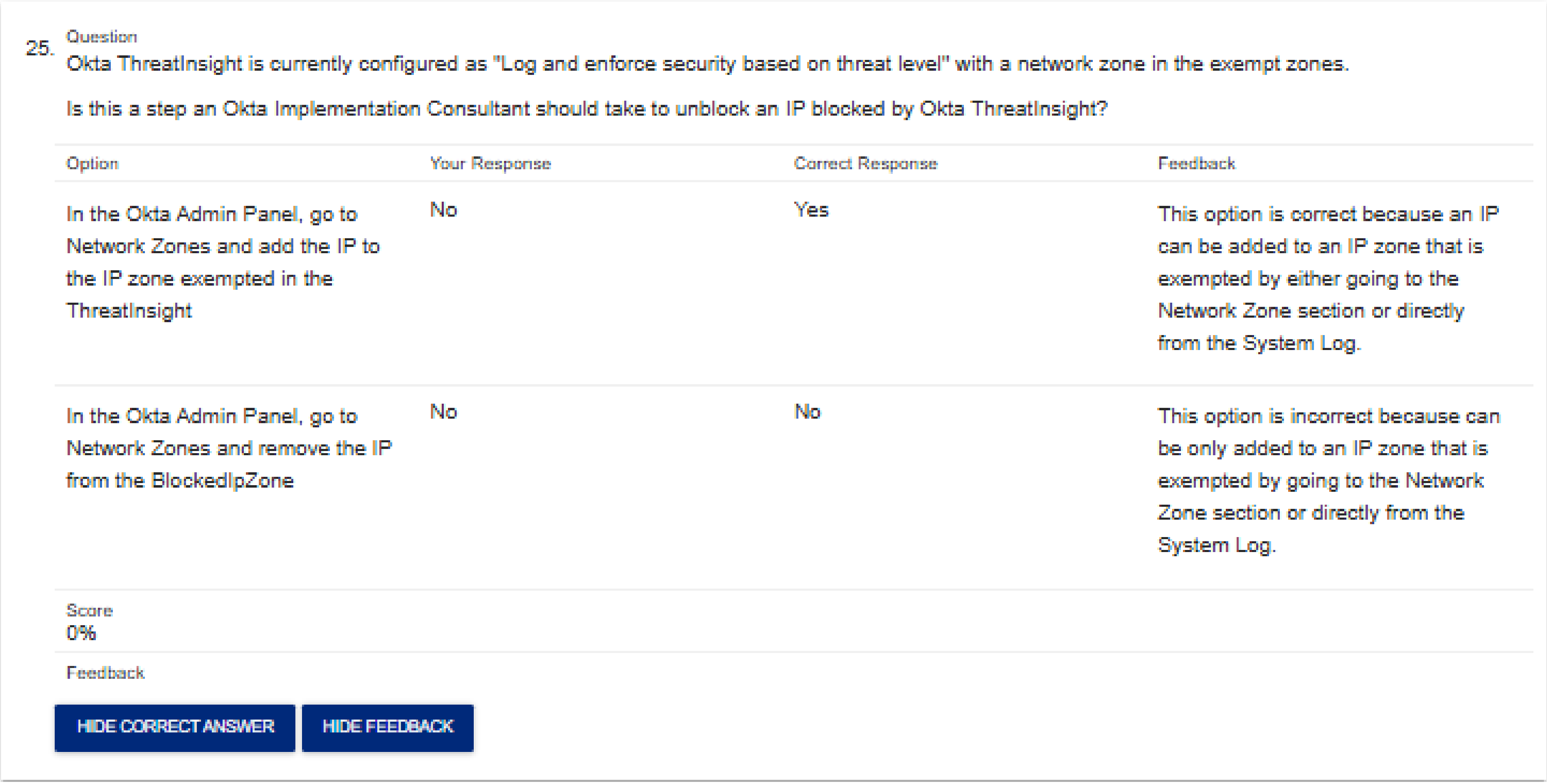
24. Question

Is this statement about the Redirect Authentication Model true?

Option	Your Response	Correct Response	Feedback
When the Redirect Authentication Deployment Model is used, the user is kept in the application, which reduces redirects to and from Okta.	No	No	This option is incorrect because when the Redirect Authentication Model is used the user or system is redirected to Okta for credential verification and is then provided authenticated access to the client application and other Service Providers.
When the Redirect Authentication Deployment Model is used, cross-site scripting (XSS) attacks on the application can result in stolen sign-in credentials.	No	No	This option is incorrect because XSS (cross-site scripting) attacks on your application do not affect the sign-in experience when using the Redirect Authentication Deployment Model.
The Redirect Authentication Deployment Model requires a greater level of effort to integrate and maintain compared to the Embedded Authentication Model.	No	No	This option is incorrect because the Embedded Authentication Model requires a higher level of effort to integrate and maintain compared to the Okta-hosted Sign-In Widget.
The Redirect Authentication Deployment Model is customizable through HTML, CSS, and JavaScript.	Yes	Yes	This option is correct because the Redirect Authentication Model is customizable through HTML, CSS, and JavaScript.

Score
100%

Feedback



25. Question

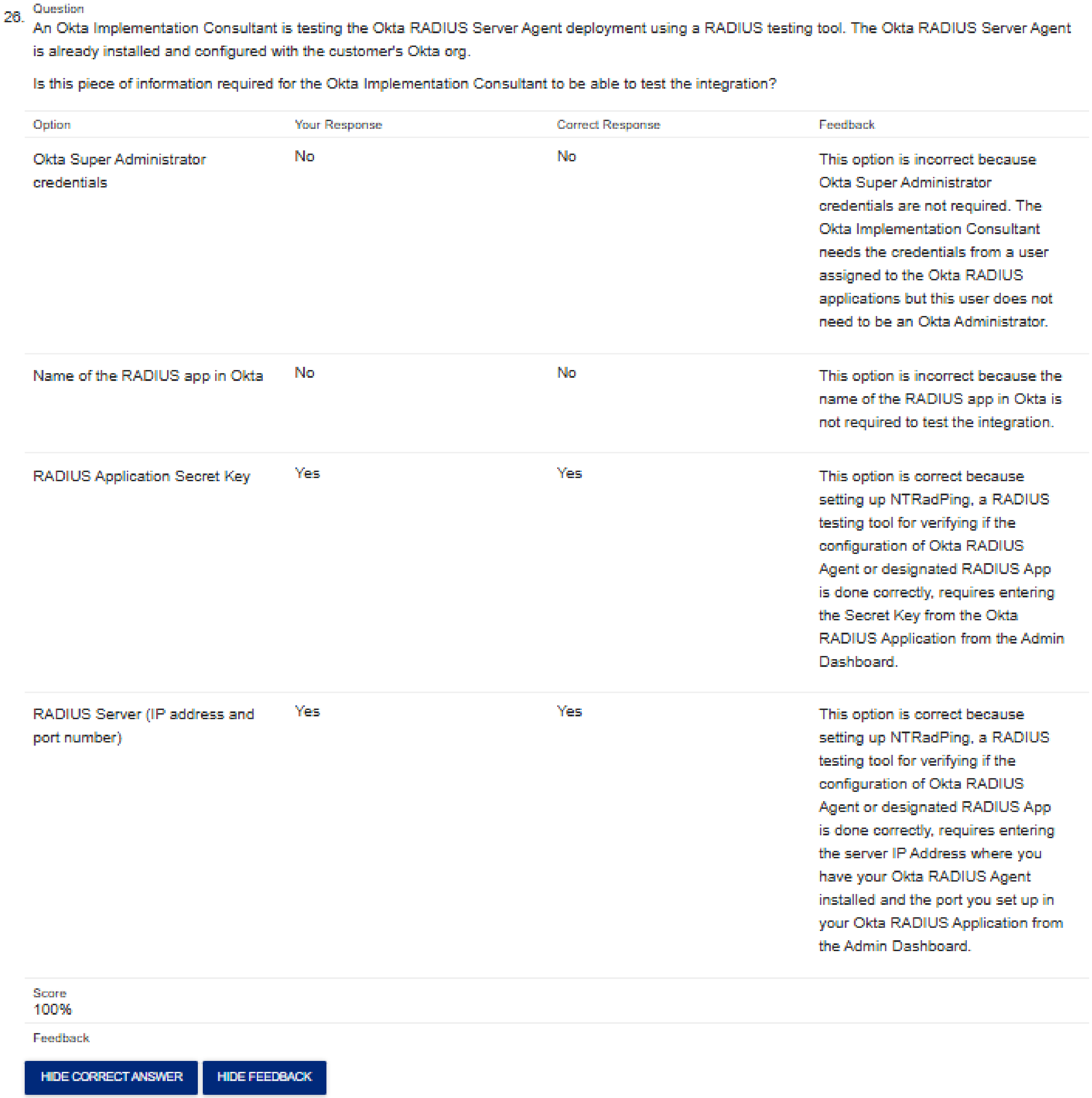
Okta ThreatInsight is currently configured as "Log and enforce security based on threat level" with a network zone in the exempt zones.

Is this a step an Okta Implementation Consultant should take to unblock an IP blocked by Okta ThreatInsight?

Option	Your Response	Correct Response	Feedback
In the Okta Admin Panel, go to Network Zones and add the IP to the IP zone exempted in the ThreatInsight	No	Yes	This option is correct because an IP can be added to an IP zone that is exempted by either going to the Network Zone section or directly from the System Log.
In the Okta Admin Panel, go to Network Zones and remove the IP from the BlockedIpZone	No	No	This option is incorrect because can be only added to an IP zone that is exempted by going to the Network Zone section or directly from the System Log.

Score
0%

Feedback



26. Question

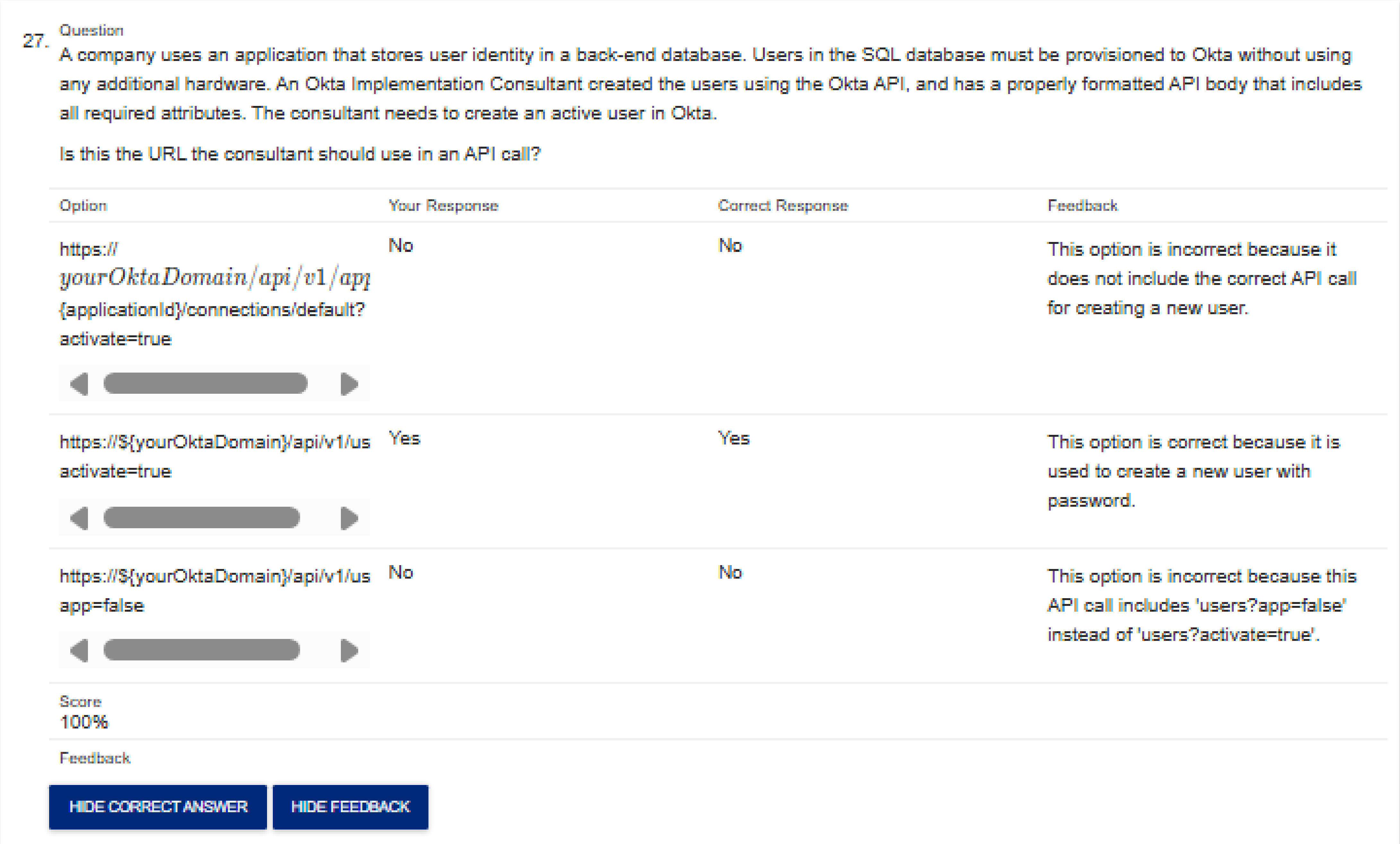
An Okta Implementation Consultant is testing the Okta RADIUS Server Agent deployment using a RADIUS testing tool. The Okta RADIUS Server Agent is already installed and configured with the customer's Okta org.

Is this piece of information required for the Okta Implementation Consultant to be able to test the integration?

Option	Your Response	Correct Response	Feedback
Okta Super Administrator credentials	No	No	This option is incorrect because Okta Super Administrator credentials are not required. The Okta Implementation Consultant needs the credentials from a user assigned to the Okta RADIUS applications but this user does not need to be an Okta Administrator.
Name of the RADIUS app in Okta	No	No	This option is incorrect because the name of the RADIUS app in Okta is not required to test the integration.
RADIUS Application Secret Key	Yes	Yes	This option is correct because setting up NTRadPing, a RADIUS testing tool for verifying if the configuration of Okta RADIUS Agent or designated RADIUS App is done correctly, requires entering the Secret Key from the Okta RADIUS Application from the Admin Dashboard.
RADIUS Server (IP address and port number)	Yes	Yes	This option is correct because setting up NTRadPing, a RADIUS testing tool for verifying if the configuration of Okta RADIUS Agent or designated RADIUS App is done correctly, requires entering the server IP Address where you have your Okta RADIUS Agent installed and the port you set up in your Okta RADIUS Application from the Admin Dashboard.

Score
100%

Feedback



27. Question

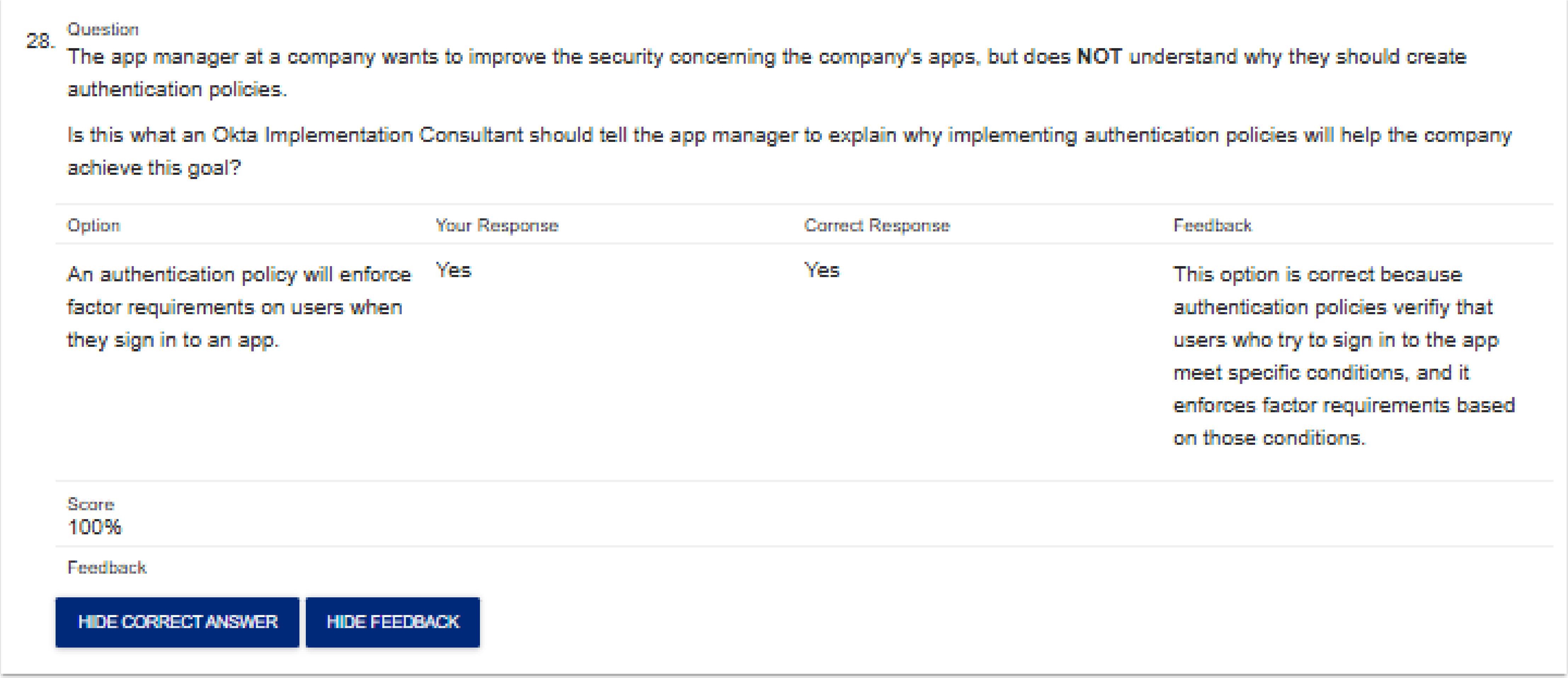
A company uses an application that stores user identity in a back-end database. Users in the SQL database must be provisioned to Okta without using any additional hardware. An Okta Implementation Consultant created the users using the Okta API, and has a properly formatted API body that includes all required attributes. The consultant needs to create an active user in Okta.

Is this the URL the consultant should use in an API call?

Option	Your Response	Correct Response	Feedback
https:// $yourOktaDomain/api/v1/ap$ {applicationId}/connections/default? activate=true	No	No	This option is incorrect because it does not include the correct API call for creating a new user.
https://${yourOktaDomain}/api/v1/us activate=true	Yes	Yes	This option is correct because it is used to create a new user with password.
https://${yourOktaDomain}/api/v1/us app=false	No	No	This option is incorrect because this API call includes 'users?app=false' instead of 'users?activate=true'.

Score
100%

Feedback



28. Question

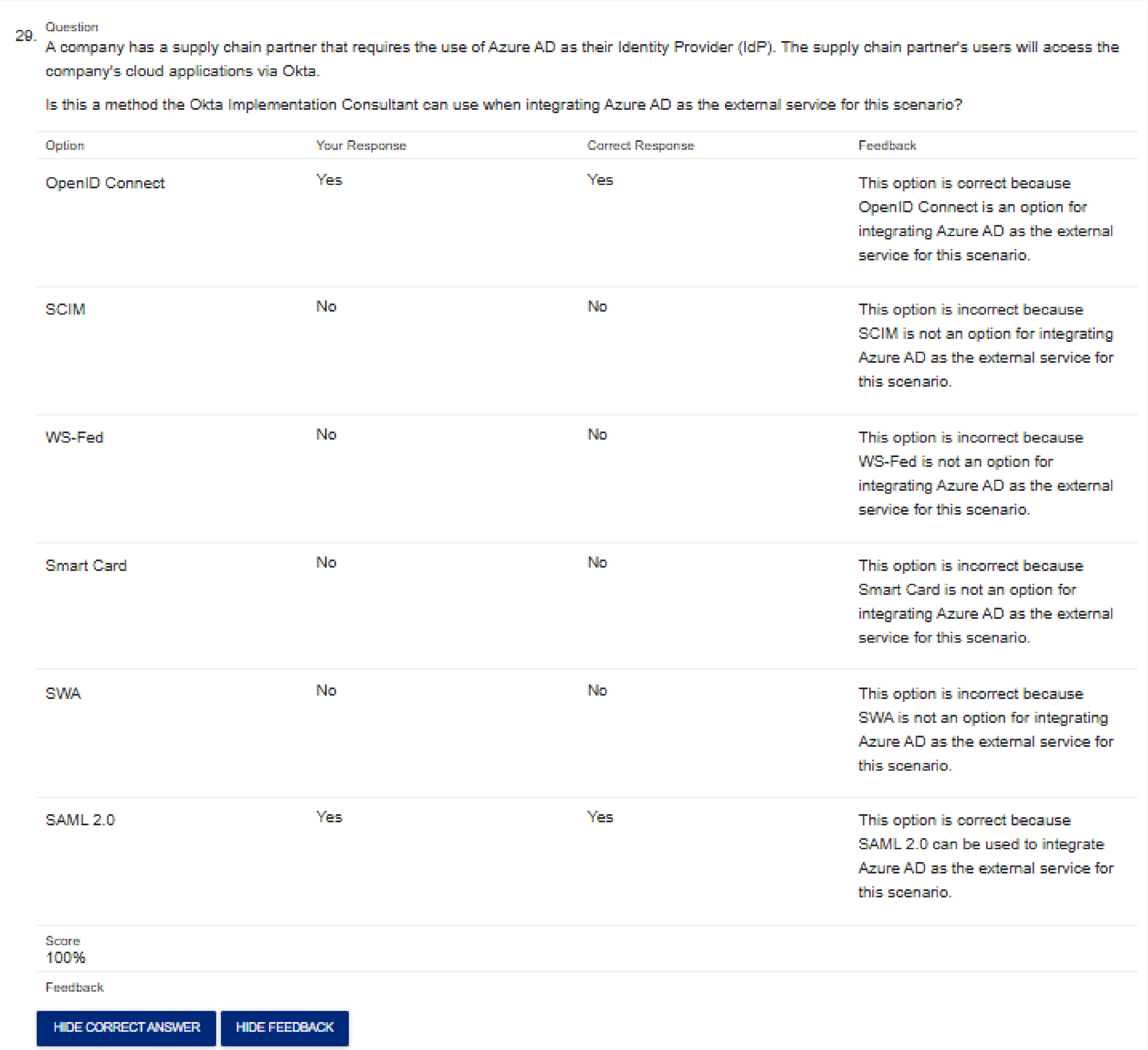
The app manager at a company wants to improve the security concerning the company's apps, but does **NOT** understand why they should create authentication policies.

Is this what an Okta Implementation Consultant should tell the app manager to explain why implementing authentication policies will help the company achieve this goal?

Option	Your Response	Correct Response	Feedback
An authentication policy will enforce factor requirements on users when they sign in to an app.	Yes	Yes	This option is correct because authentication policies verifiy that users who try to sign in to the app meet specific conditions, and it enforces factor requirements based on those conditions.

Score
100%

Feedback



29. Question

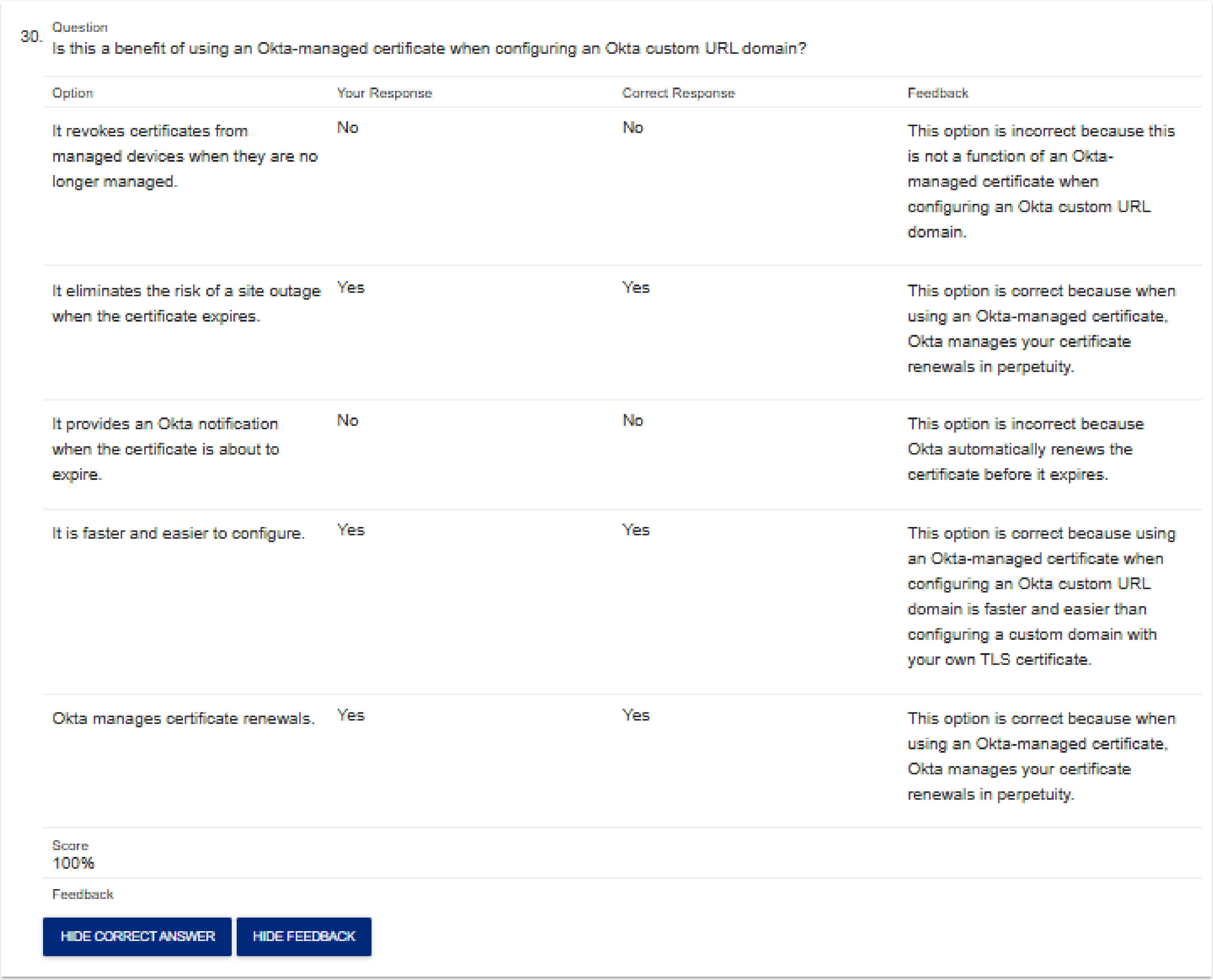
A company has a supply chain partner that requires the use of Azure AD as their Identity Provider (IdP). The supply chain partner's users will access the company's cloud applications via Okta.

Is this a method the Okta Implementation Consultant can use when integrating Azure AD as the external service for this scenario?

Option	Your Response	Correct Response	Feedback
OpenID Connect	Yes	Yes	This option is correct because OpenID Connect is an option for integrating Azure AD as the external service for this scenario.
SCIM	No	No	This option is incorrect because SCIM is not an option for integrating Azure AD as the external service for this scenario.
WS-Fed	No	No	This option is incorrect because WS-Fed is not an option for integrating Azure AD as the external service for this scenario.
Smart Card	No	No	This option is incorrect because Smart Card is not an option for integrating Azure AD as the external service for this scenario.
SWA	No	No	This option is incorrect because SWA is not an option for integrating Azure AD as the external service for this scenario.
SAML 2.0	Yes	Yes	This option is correct because SAML 2.0 can be used to integrate Azure AD as the external service for this scenario.

Score
100%

Feedback



30. Question

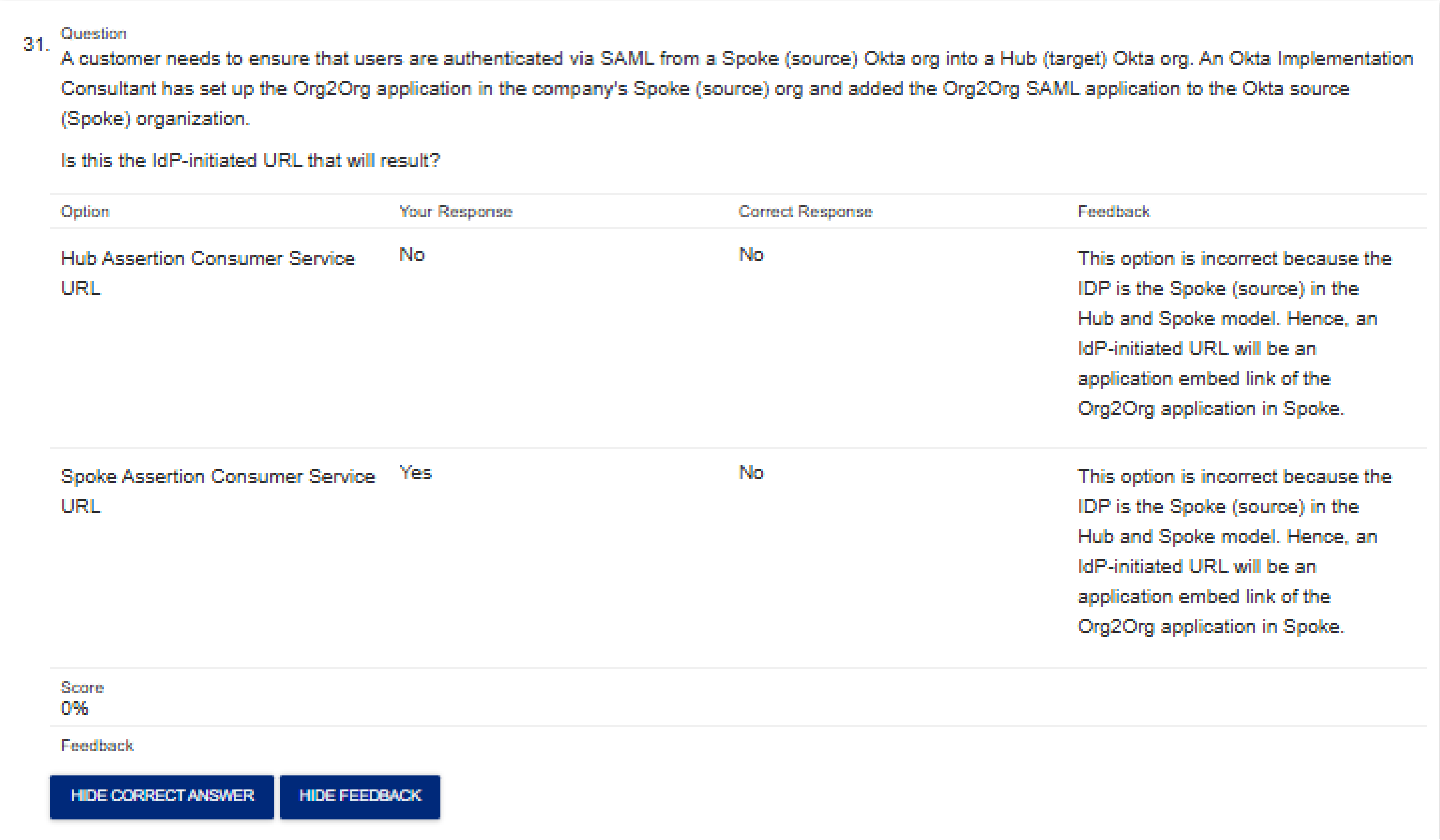
Is this a benefit of using an Okta-managed certificate when configuring an Okta custom URL domain?

Option	Your Response	Correct Response	Feedback
It revokes certificates from managed devices when they are no longer managed.	No	No	This option is incorrect because this is not a function of an Okta-managed certificate when configuring an Okta custom URL domain.
It eliminates the risk of a site outage when the certificate expires.	Yes	Yes	This option is correct because when using an Okta-managed certificate, Okta manages your certificate renewals in perpetuity.
It provides an Okta notification when the certificate is about to expire.	No	No	This option is incorrect because Okta automatically renews the certificate before it expires.
It is faster and easier to configure.	Yes	Yes	This option is correct because using an Okta-managed certificate when configuring an Okta custom URL domain is faster and easier than configuring a custom domain with your own TLS certificate.
Okta manages certificate renewals.	Yes	Yes	This option is correct because when using an Okta-managed certificate, Okta manages your certificate renewals in perpetuity.

Score

100%

Feedback



31. Question

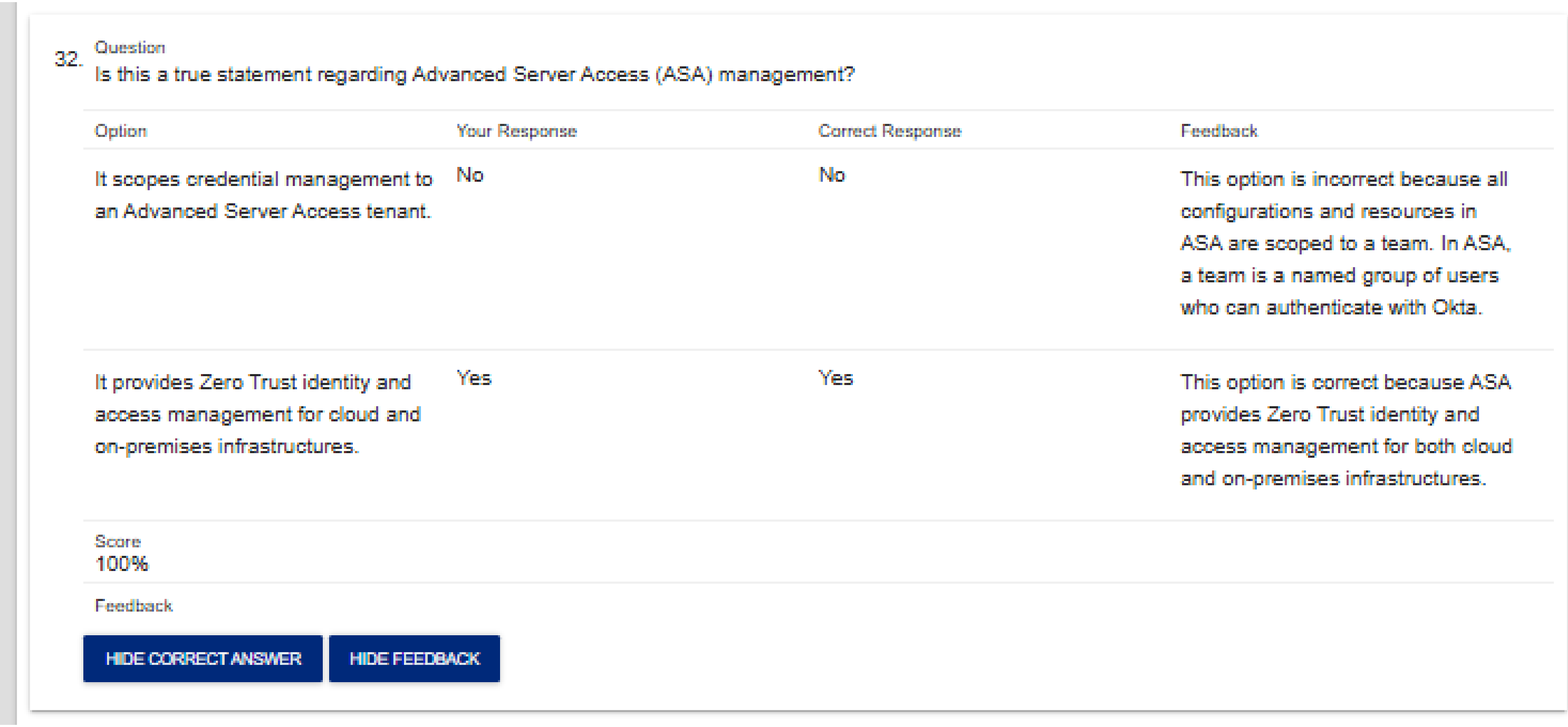
A customer needs to ensure that users are authenticated via SAML from a Spoke (source) Okta org into a Hub (target) Okta org. An Okta Implementation Consultant has set up the Org2Org application in the company's Spoke (source) org and added the Org2Org SAML application to the Okta source (Spoke) organization.

Is this the IdP-initiated URL that will result?

Option	Your Response	Correct Response	Feedback
Hub Assertion Consumer Service URL	No	No	This option is incorrect because the IDP is the Spoke (source) in the Hub and Spoke model. Hence, an IdP-initiated URL will be an application embed link of the Org2Org application in Spoke.
Spoke Assertion Consumer Service URL	Yes	No	This option is incorrect because the IDP is the Spoke (source) in the Hub and Spoke model. Hence, an IdP-initiated URL will be an application embed link of the Org2Org application in Spoke.

Score
0%

Feedback



32. Question

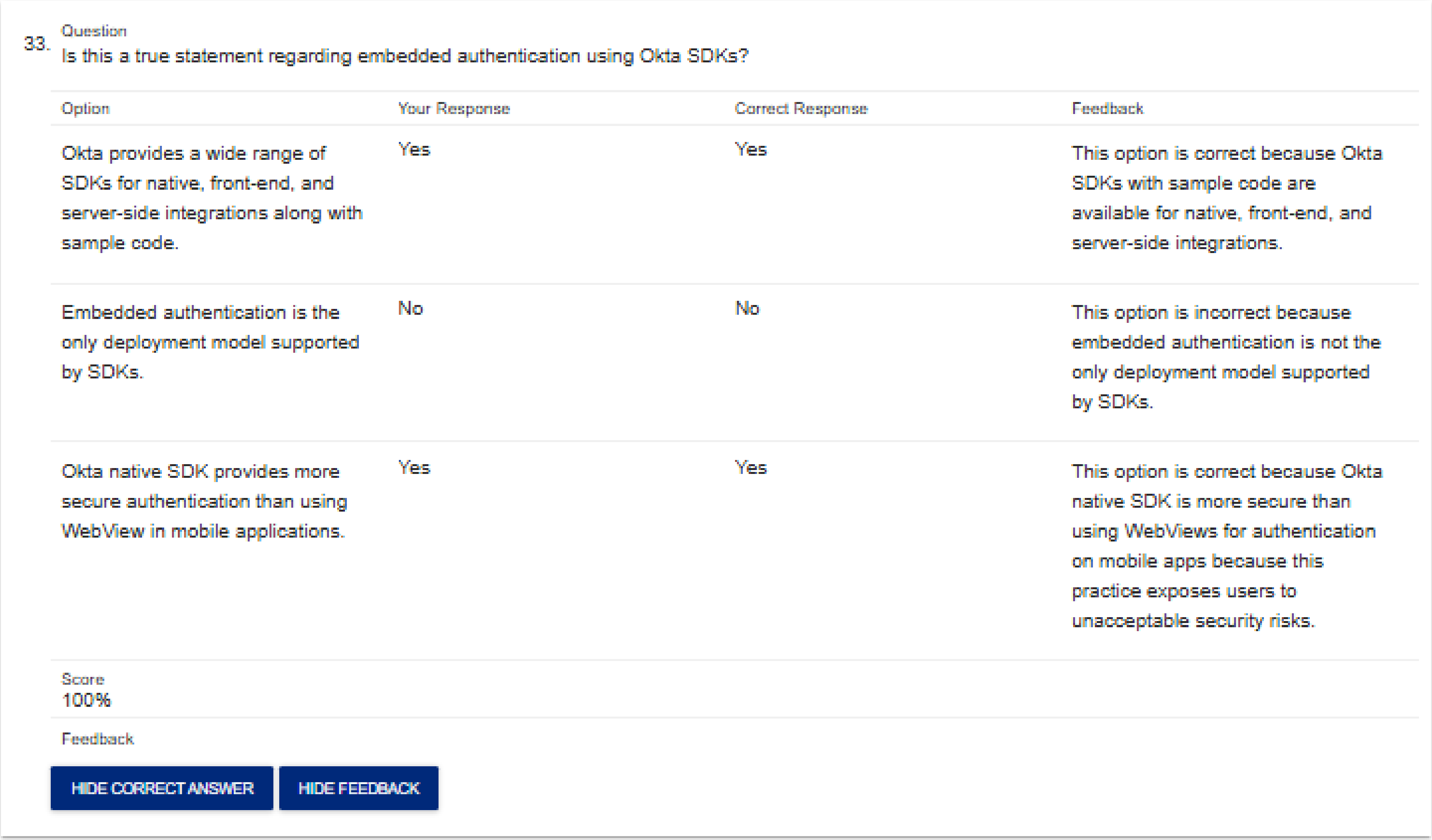
Is this a true statement regarding Advanced Server Access (ASA) management?

Option	Your Response	Correct Response	Feedback
It scopes credential management to an Advanced Server Access tenant.	No	No	This option is incorrect because all configurations and resources in ASA are scoped to a team. In ASA, a team is a named group of users who can authenticate with Okta.
It provides Zero Trust identity and access management for cloud and on-premises infrastructures.	Yes	Yes	This option is correct because ASA provides Zero Trust identity and access management for both cloud and on-premises infrastructures.

Score

100%

Feedback



33. Question

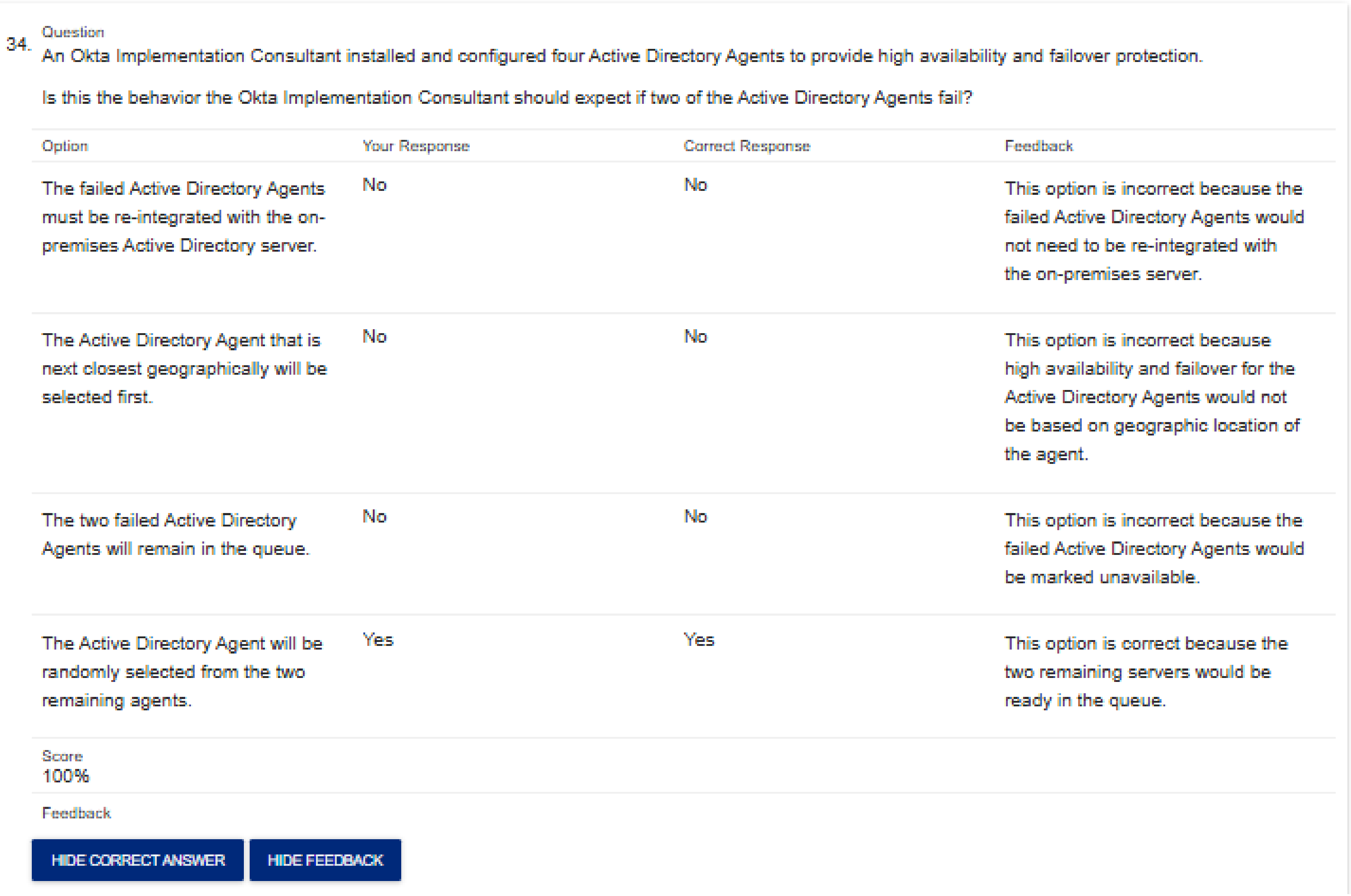
Is this a true statement regarding embedded authentication using Okta SDKs?

Option	Your Response	Correct Response	Feedback
Okta provides a wide range of SDKs for native, front-end, and server-side integrations along with sample code.	Yes	Yes	This option is correct because Okta SDKs with sample code are available for native, front-end, and server-side integrations.
Embedded authentication is the only deployment model supported by SDKs.	No	No	This option is incorrect because embedded authentication is not the only deployment model supported by SDKs.
Okta native SDK provides more secure authentication than using WebView in mobile applications.	Yes	Yes	This option is correct because Okta native SDK is more secure than using WebViews for authentication on mobile apps because this practice exposes users to unacceptable security risks.

Score

100%

Feedback



34. Question

An Okta Implementation Consultant installed and configured four Active Directory Agents to provide high availability and failover protection.

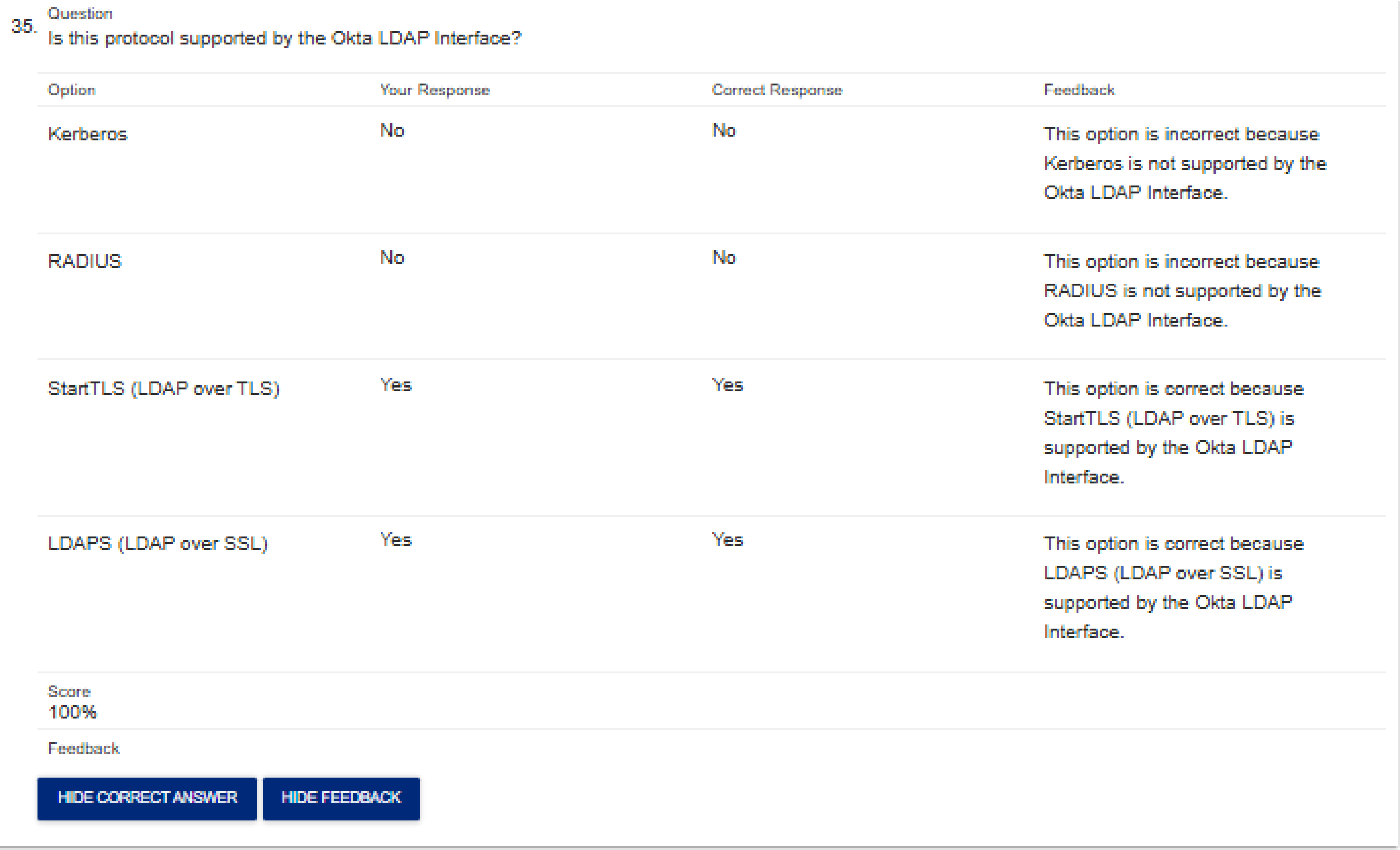
Is this the behavior the Okta Implementation Consultant should expect if two of the Active Directory Agents fail?

Option	Your Response	Correct Response	Feedback
The failed Active Directory Agents must be re-integrated with the on-premises Active Directory server.	No	No	This option is incorrect because the failed Active Directory Agents would not need to be re-integrated with the on-premises server.
The Active Directory Agent that is next closest geographically will be selected first.	No	No	This option is incorrect because high availability and failover for the Active Directory Agents would not be based on geographic location of the agent.
The two failed Active Directory Agents will remain in the queue.	No	No	This option is incorrect because the failed Active Directory Agents would be marked unavailable.
The Active Directory Agent will be randomly selected from the two remaining agents.	Yes	Yes	This option is correct because the two remaining servers would be ready in the queue.

Score

100%

Feedback



35. Question

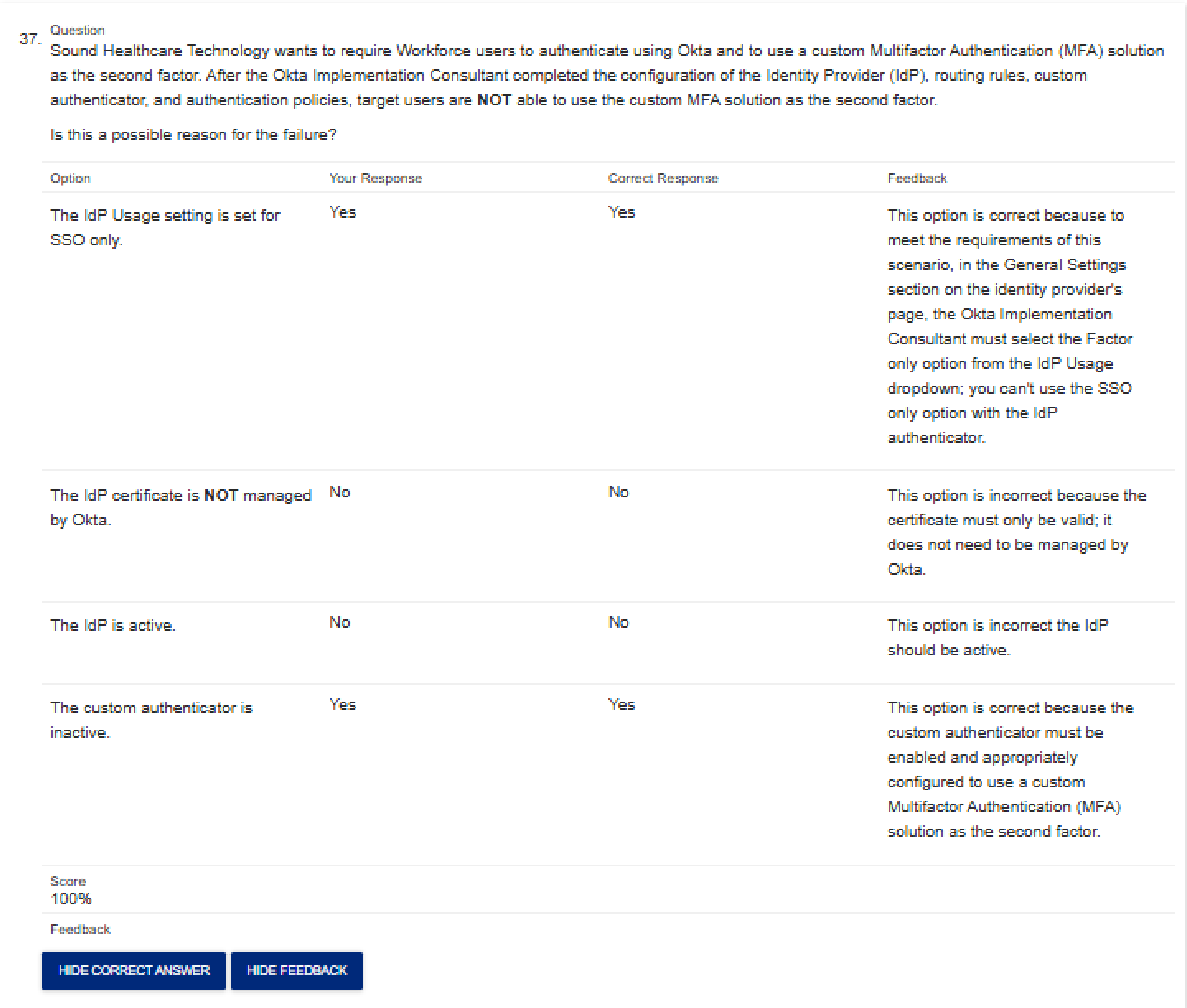
Is this protocol supported by the Okta LDAP Interface?

Option	Your Response	Correct Response	Feedback
Kerberos	No	No	This option is incorrect because Kerberos is not supported by the Okta LDAP Interface.
RADIUS	No	No	This option is incorrect because RADIUS is not supported by the Okta LDAP Interface.
StartTLS (LDAP over TLS)	Yes	Yes	This option is correct because StartTLS (LDAP over TLS) is supported by the Okta LDAP Interface.
LDAPS (LDAP over SSL)	Yes	Yes	This option is correct because LDAPS (LDAP over SSL) is supported by the Okta LDAP Interface.

Score

100%

Feedback



37. Question

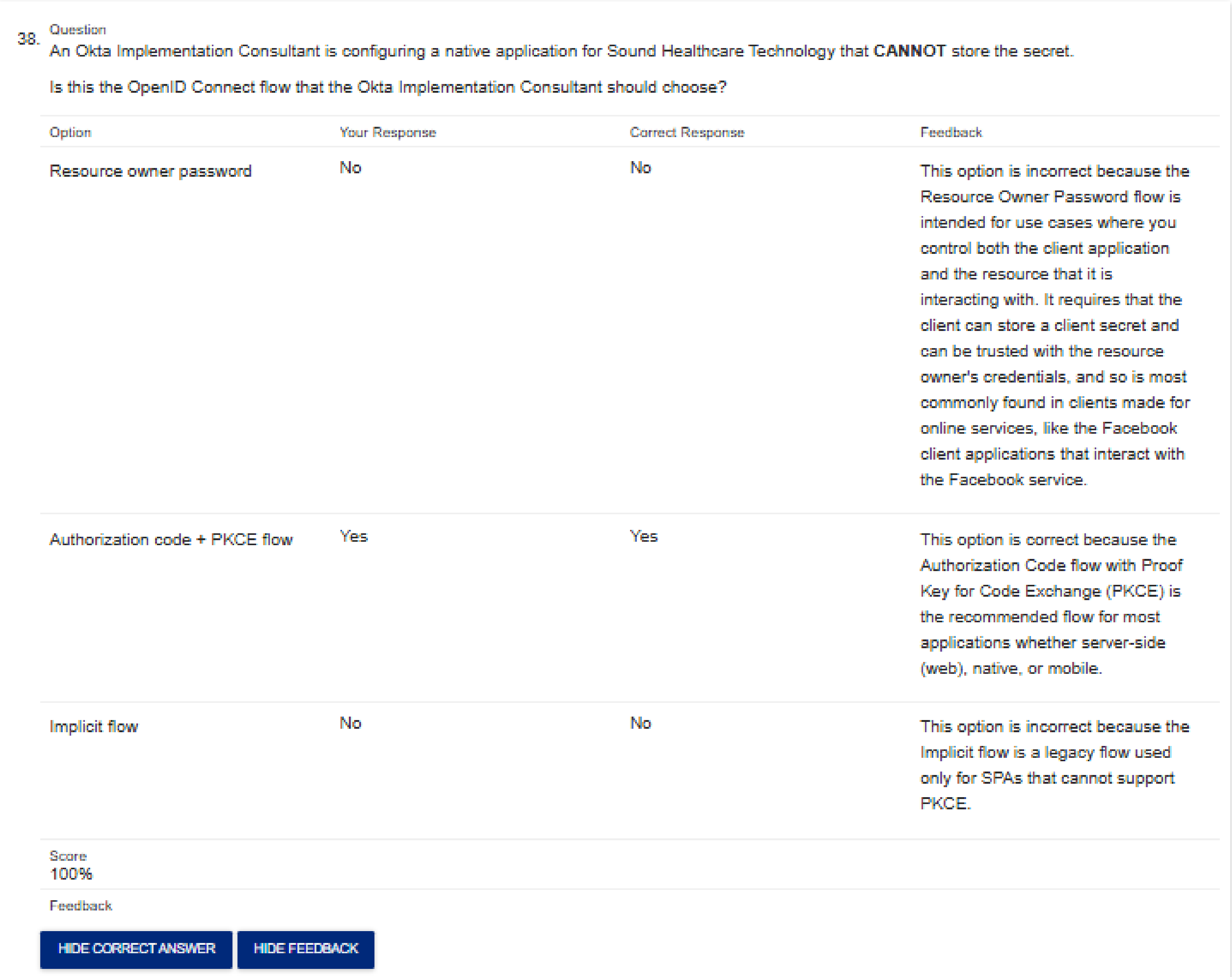
Sound Healthcare Technology wants to require Workforce users to authenticate using Okta and to use a custom Multifactor Authentication (MFA) solution as the second factor. After the Okta Implementation Consultant completed the configuration of the Identity Provider (IdP), routing rules, custom authenticator, and authentication policies, target users are **NOT** able to use the custom MFA solution as the second factor.

Is this a possible reason for the failure?

Option	Your Response	Correct Response	Feedback
The IdP Usage setting is set for SSO only.	Yes	Yes	This option is correct because to meet the requirements of this scenario, in the General Settings section on the identity provider's page, the Okta Implementation Consultant must select the Factor only option from the IdP Usage dropdown; you can't use the SSO only option with the IdP authenticator.
The IdP certificate is **NOT** managed by Okta.	No	No	This option is incorrect because the certificate must only be valid; it does not need to be managed by Okta.
The IdP is active.	No	No	This option is incorrect the IdP should be active.
The custom authenticator is inactive.	Yes	Yes	This option is correct because the custom authenticator must be enabled and appropriately configured to use a custom Multifactor Authentication (MFA) solution as the second factor.

Score
100%

Feedback



38. Question

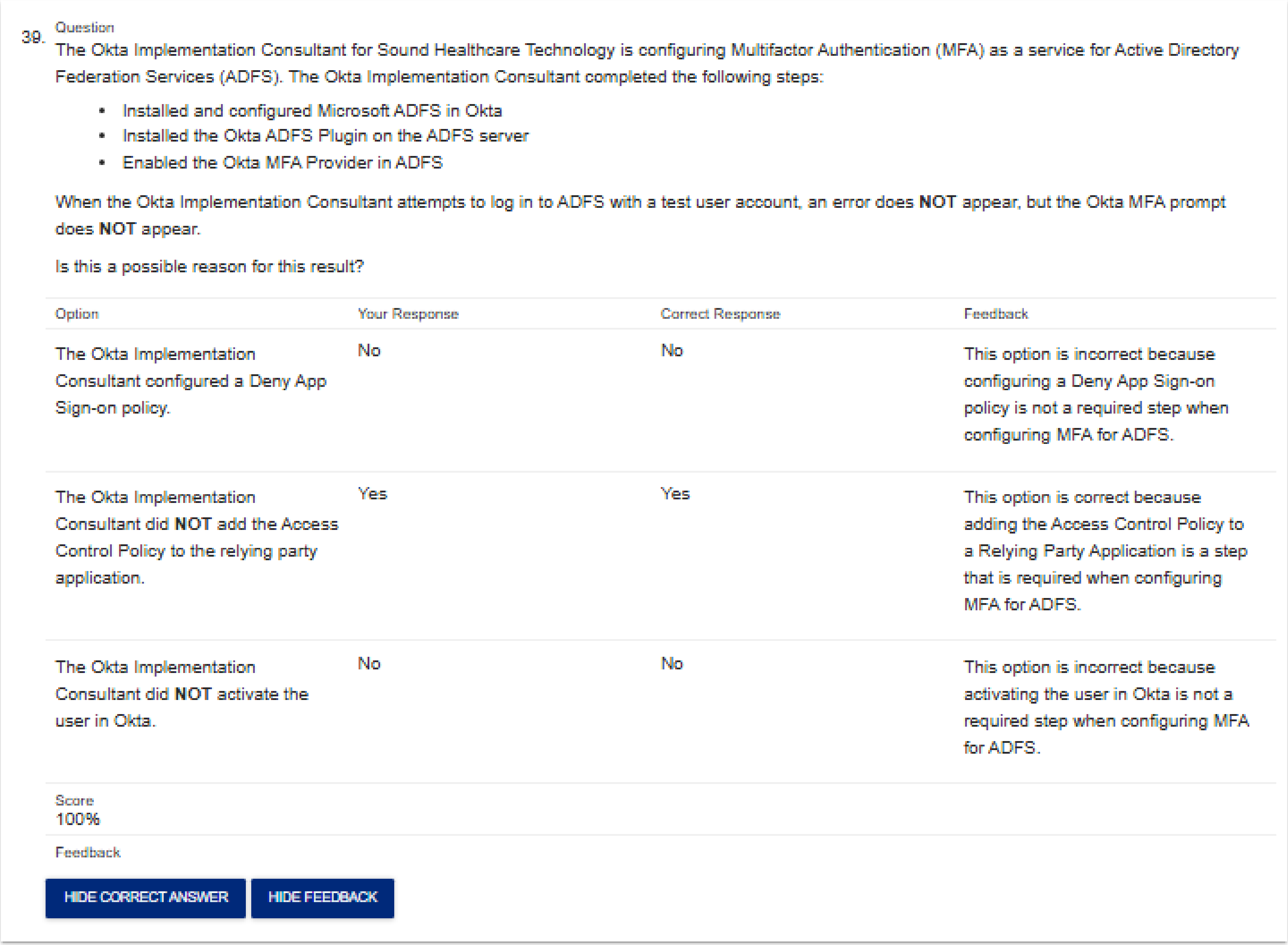
An Okta Implementation Consultant is configuring a native application for Sound Healthcare Technology that **CANNOT** store the secret.

Is this the OpenID Connect flow that the Okta Implementation Consultant should choose?

Option	Your Response	Correct Response	Feedback
Resource owner password	No	No	This option is incorrect because the Resource Owner Password flow is intended for use cases where you control both the client application and the resource that it is interacting with. It requires that the client can store a client secret and can be trusted with the resource owner's credentials, and so is most commonly found in clients made for online services, like the Facebook client applications that interact with the Facebook service.
Authorization code + PKCE flow	Yes	Yes	This option is correct because the Authorization Code flow with Proof Key for Code Exchange (PKCE) is the recommended flow for most applications whether server-side (web), native, or mobile.
Implicit flow	No	No	This option is incorrect because the Implicit flow is a legacy flow used only for SPAs that cannot support PKCE.

Score
100%

Feedback



39. Question

The Okta Implementation Consultant for Sound Healthcare Technology is configuring Multifactor Authentication (MFA) as a service for Active Directory Federation Services (ADFS). The Okta Implementation Consultant completed the following steps:

- Installed and configured Microsoft ADFS in Okta
- Installed the Okta ADFS Plugin on the ADFS server
- Enabled the Okta MFA Provider in ADFS

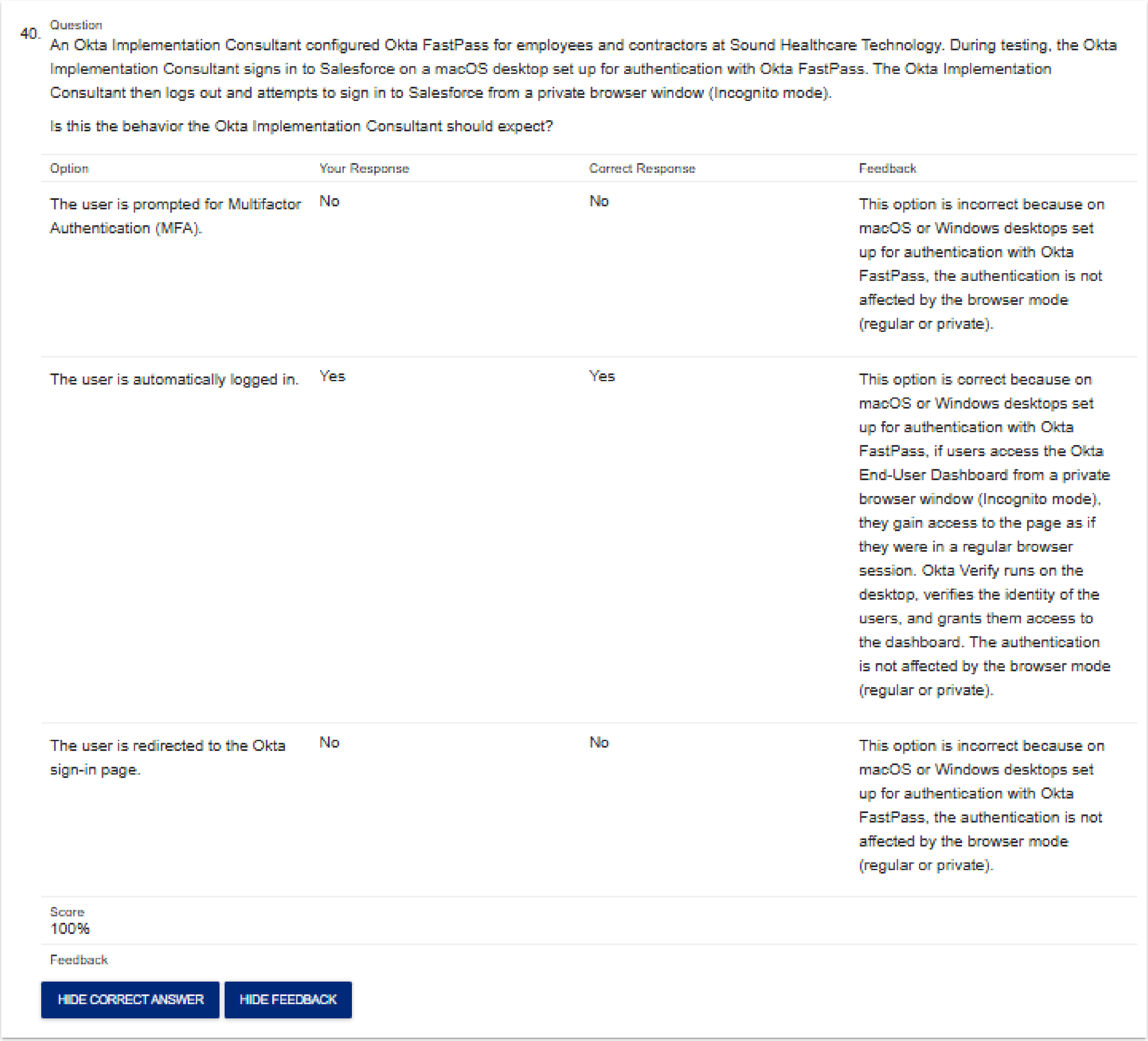
When the Okta Implementation Consultant attempts to log in to ADFS with a test user account, an error does **NOT** appear, but the Okta MFA prompt does **NOT** appear.

Is this a possible reason for this result?

Option	Your Response	Correct Response	Feedback
The Okta Implementation Consultant configured a Deny App Sign-on policy.	No	No	This option is incorrect because configuring a Deny App Sign-on policy is not a required step when configuring MFA for ADFS.
The Okta Implementation Consultant did **NOT** add the Access Control Policy to the relying party application.	Yes	Yes	This option is correct because adding the Access Control Policy to a Relying Party Application is a step that is required when configuring MFA for ADFS.
The Okta Implementation Consultant did **NOT** activate the user in Okta.	No	No	This option is incorrect because activating the user in Okta is not a required step when configuring MFA for ADFS.

Score
100%

Feedback



40. Question

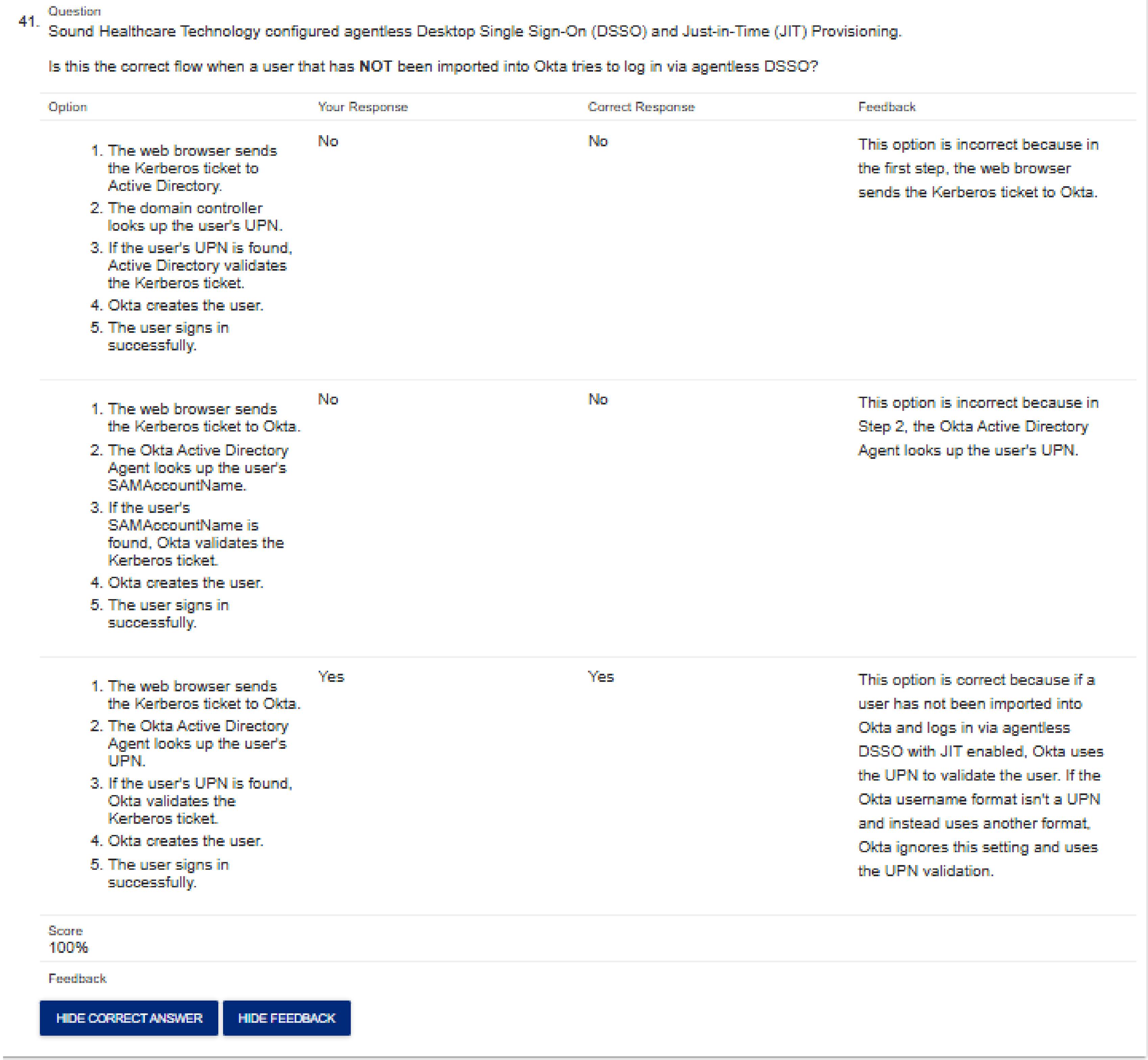
An Okta Implementation Consultant configured Okta FastPass for employees and contractors at Sound Healthcare Technology. During testing, the Okta Implementation Consultant signs in to Salesforce on a macOS desktop set up for authentication with Okta FastPass. The Okta Implementation Consultant then logs out and attempts to sign in to Salesforce from a private browser window (Incognito mode).

Is this the behavior the Okta Implementation Consultant should expect?

Option	Your Response	Correct Response	Feedback
The user is prompted for Multifactor Authentication (MFA).	No	No	This option is incorrect because on macOS or Windows desktops set up for authentication with Okta FastPass, the authentication is not affected by the browser mode (regular or private).
The user is automatically logged in.	Yes	Yes	This option is correct because on macOS or Windows desktops set up for authentication with Okta FastPass, if users access the Okta End-User Dashboard from a private browser window (Incognito mode), they gain access to the page as if they were in a regular browser session. Okta Verify runs on the desktop, verifies the identity of the users, and grants them access to the dashboard. The authentication is not affected by the browser mode (regular or private).
The user is redirected to the Okta sign-in page.	No	No	This option is incorrect because on macOS or Windows desktops set up for authentication with Okta FastPass, the authentication is not affected by the browser mode (regular or private).

Score
100%

Feedback



Question

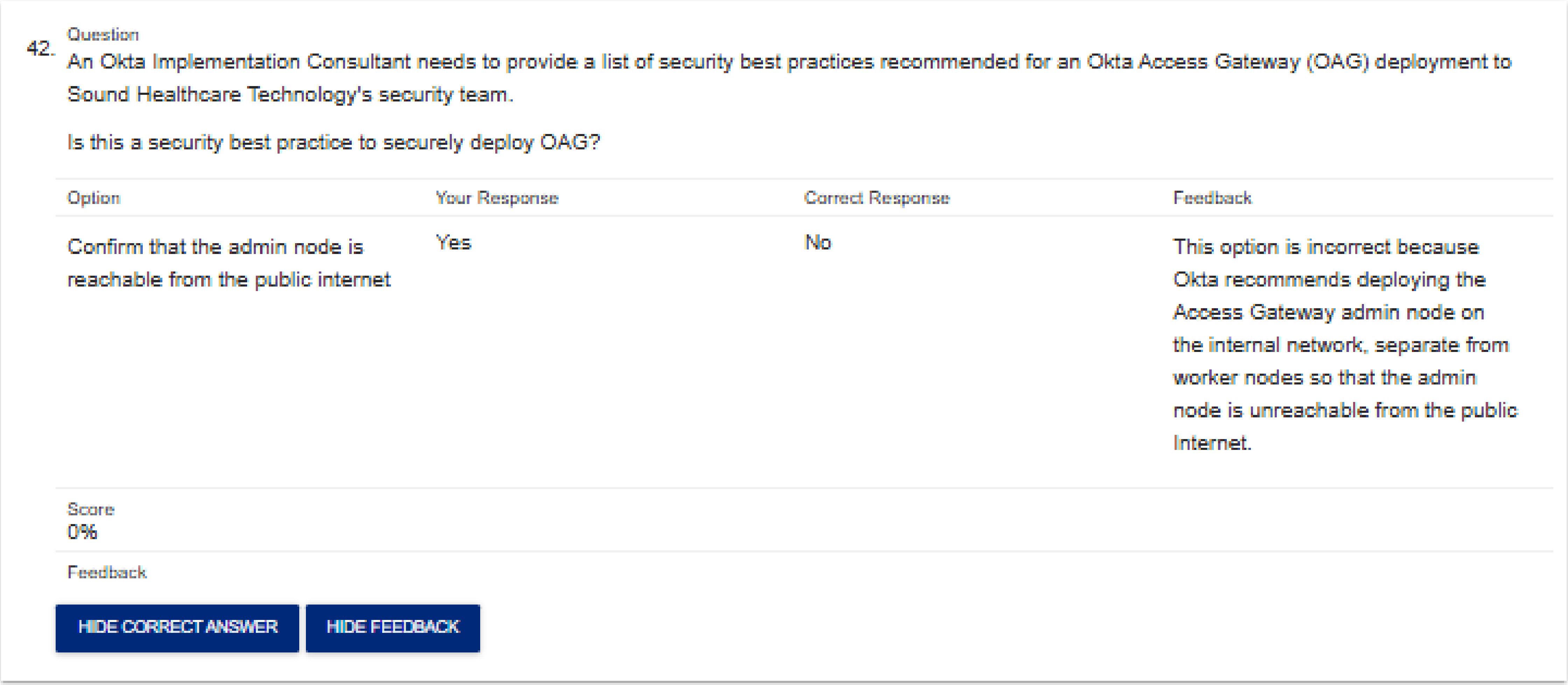
41. Sound Healthcare Technology configured agentless Desktop Single Sign-On (DSSO) and Just-in-Time (JIT) Provisioning.

Is this the correct flow when a user that has **NOT** been imported into Okta tries to log in via agentless DSSO?

Option	Your Response	Correct Response	Feedback
1. The web browser sends the Kerberos ticket to Active Directory. 2. The domain controller looks up the user's UPN. 3. If the user's UPN is found, Active Directory validates the Kerberos ticket. 4. Okta creates the user. 5. The user signs in successfully.	No	No	This option is incorrect because in the first step, the web browser sends the Kerberos ticket to Okta.
1. The web browser sends the Kerberos ticket to Okta. 2. The Okta Active Directory Agent looks up the user's SAMAccountName. 3. If the user's SAMAccountName is found, Okta validates the Kerberos ticket. 4. Okta creates the user. 5. The user signs in successfully.	No	No	This option is incorrect because in Step 2, the Okta Active Directory Agent looks up the user's UPN.
1. The web browser sends the Kerberos ticket to Okta. 2. The Okta Active Directory Agent looks up the user's UPN. 3. If the user's UPN is found, Okta validates the Kerberos ticket. 4. Okta creates the user. 5. The user signs in successfully.	Yes	Yes	This option is correct because if a user has not been imported into Okta and logs in via agentless DSSO with JIT enabled, Okta uses the UPN to validate the user. If the Okta username format isn't a UPN and instead uses another format, Okta ignores this setting and uses the UPN validation.

Score
100%

Feedback



42. Question

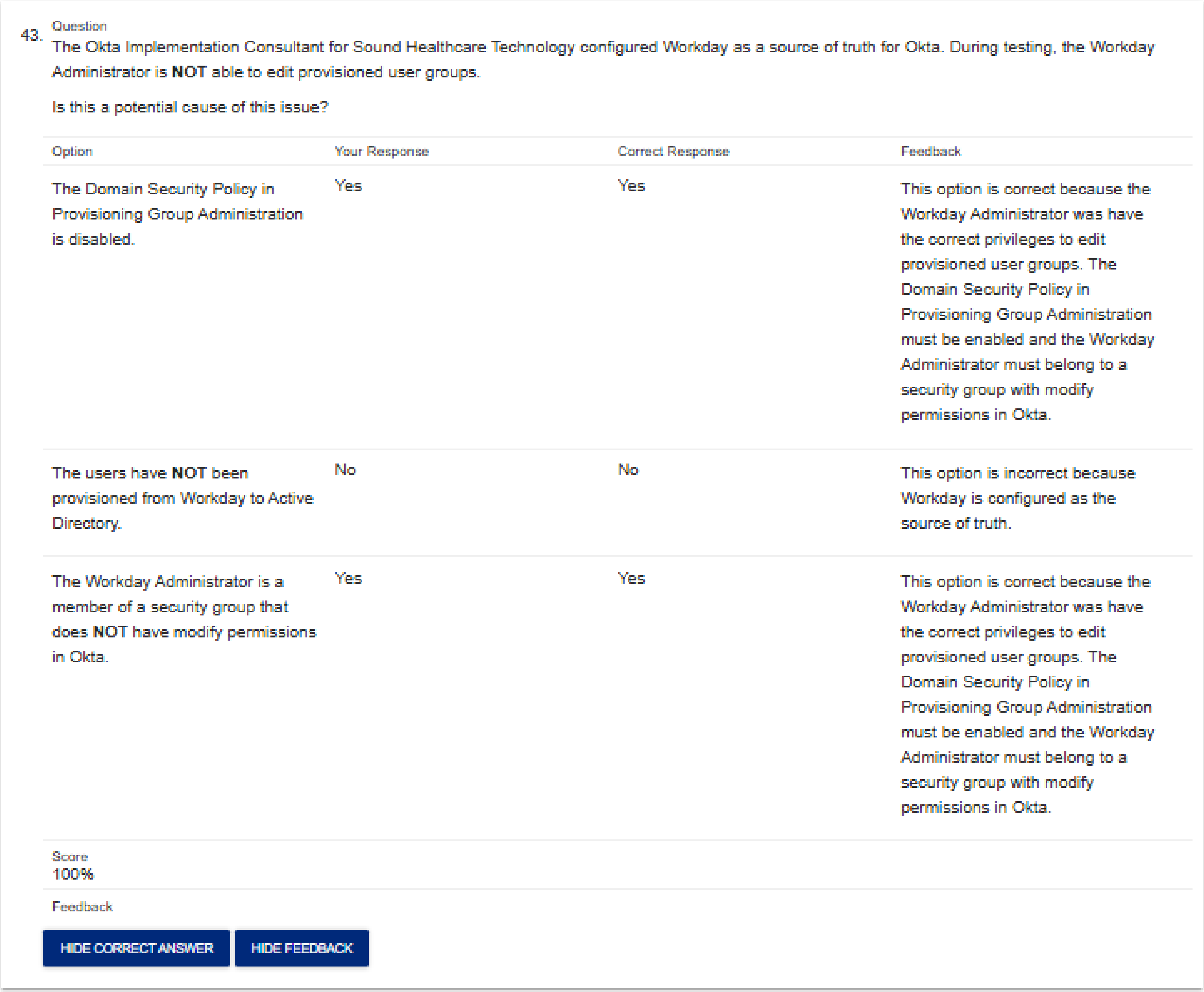
An Okta Implementation Consultant needs to provide a list of security best practices recommended for an Okta Access Gateway (OAG) deployment to Sound Healthcare Technology's security team.

Is this a security best practice to securely deploy OAG?

Option	Your Response	Correct Response	Feedback
Confirm that the admin node is reachable from the public internet	Yes	No	This option is incorrect because Okta recommends deploying the Access Gateway admin node on the internal network, separate from worker nodes so that the admin node is unreachable from the public Internet.

Score
0%

Feedback



43. Question

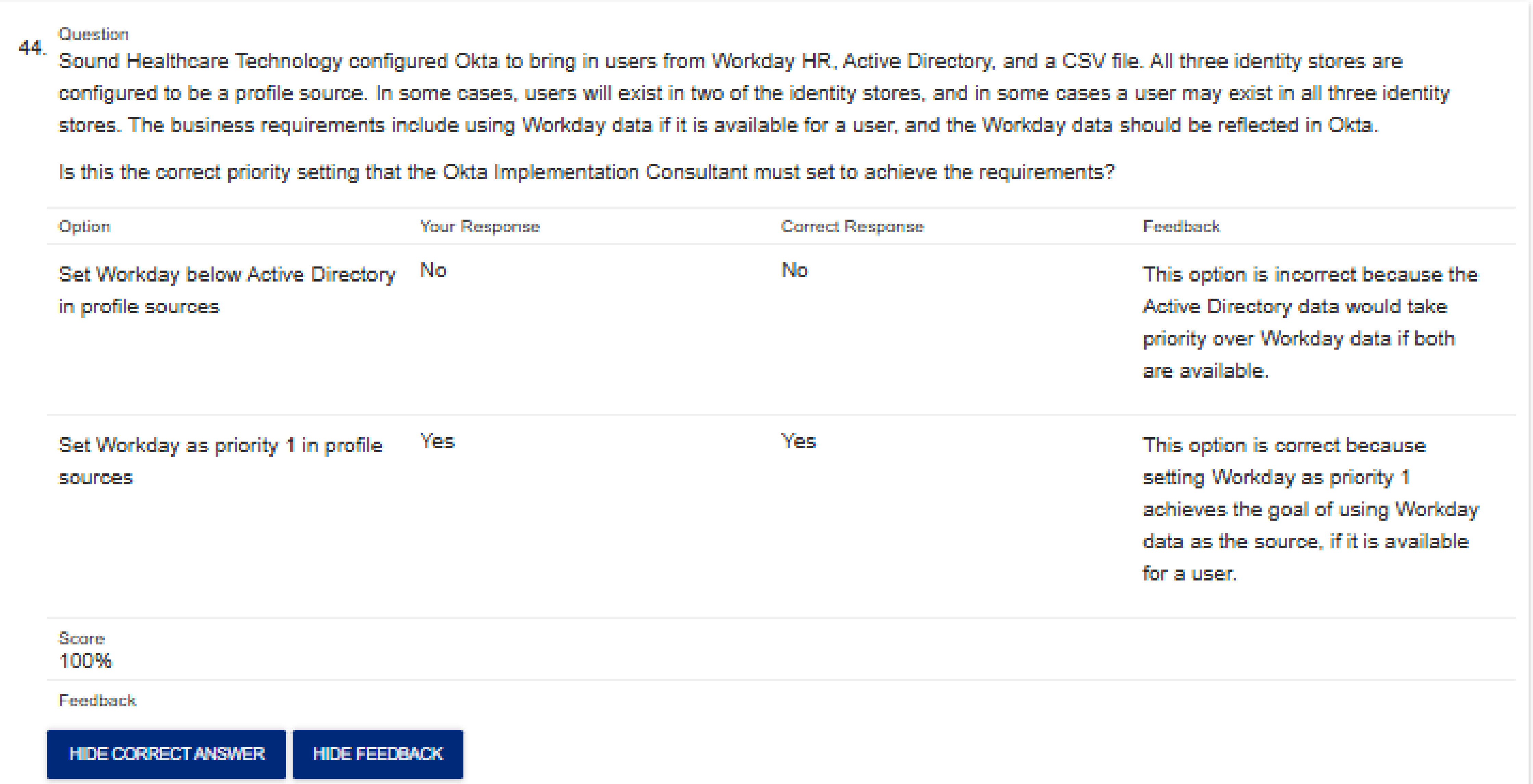
The Okta Implementation Consultant for Sound Healthcare Technology configured Workday as a source of truth for Okta. During testing, the Workday Administrator is **NOT** able to edit provisioned user groups.

Is this a potential cause of this issue?

Option	Your Response	Correct Response	Feedback
The Domain Security Policy in Provisioning Group Administration is disabled.	Yes	Yes	This option is correct because the Workday Administrator was have the correct privileges to edit provisioned user groups. The Domain Security Policy in Provisioning Group Administration must be enabled and the Workday Administrator must belong to a security group with modify permissions in Okta.
The users have **NOT** been provisioned from Workday to Active Directory.	No	No	This option is incorrect because Workday is configured as the source of truth.
The Workday Administrator is a member of a security group that does **NOT** have modify permissions in Okta.	Yes	Yes	This option is correct because the Workday Administrator was have the correct privileges to edit provisioned user groups. The Domain Security Policy in Provisioning Group Administration must be enabled and the Workday Administrator must belong to a security group with modify permissions in Okta.

Score
100%

Feedback



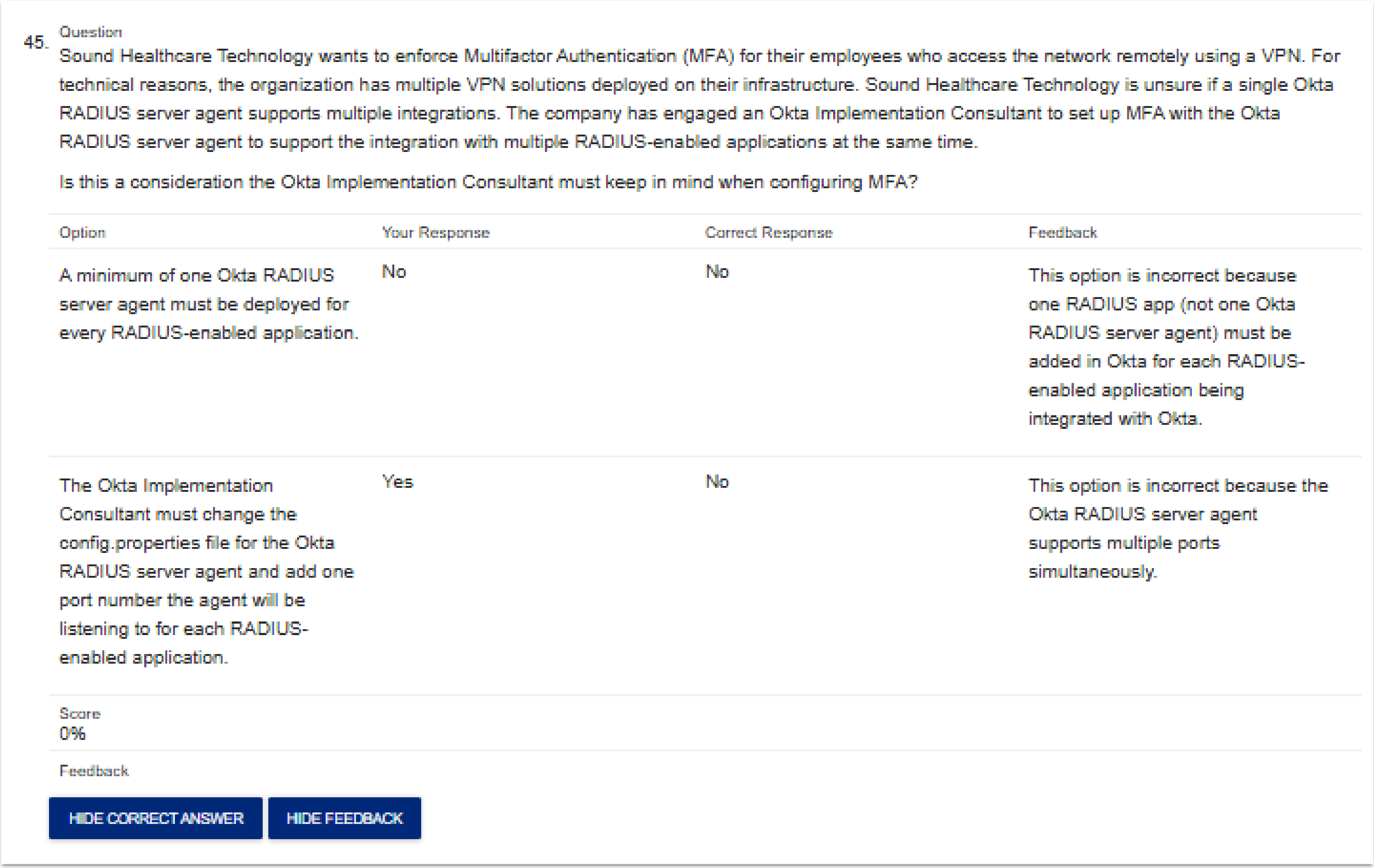
44. Sound Healthcare Technology configured Okta to bring in users from Workday HR, Active Directory, and a CSV file. All three identity stores are configured to be a profile source. In some cases, users will exist in two of the identity stores, and in some cases a user may exist in all three identity stores. The business requirements include using Workday data if it is available for a user, and the Workday data should be reflected in Okta.

Is this the correct priority setting that the Okta Implementation Consultant must set to achieve the requirements?

Option	Your Response	Correct Response	Feedback
Set Workday below Active Directory in profile sources	No	No	This option is incorrect because the Active Directory data would take priority over Workday data if both are available.
Set Workday as priority 1 in profile sources	Yes	Yes	This option is correct because setting Workday as priority 1 achieves the goal of using Workday data as the source, if it is available for a user.

Score
100%

Feedback



45. Question

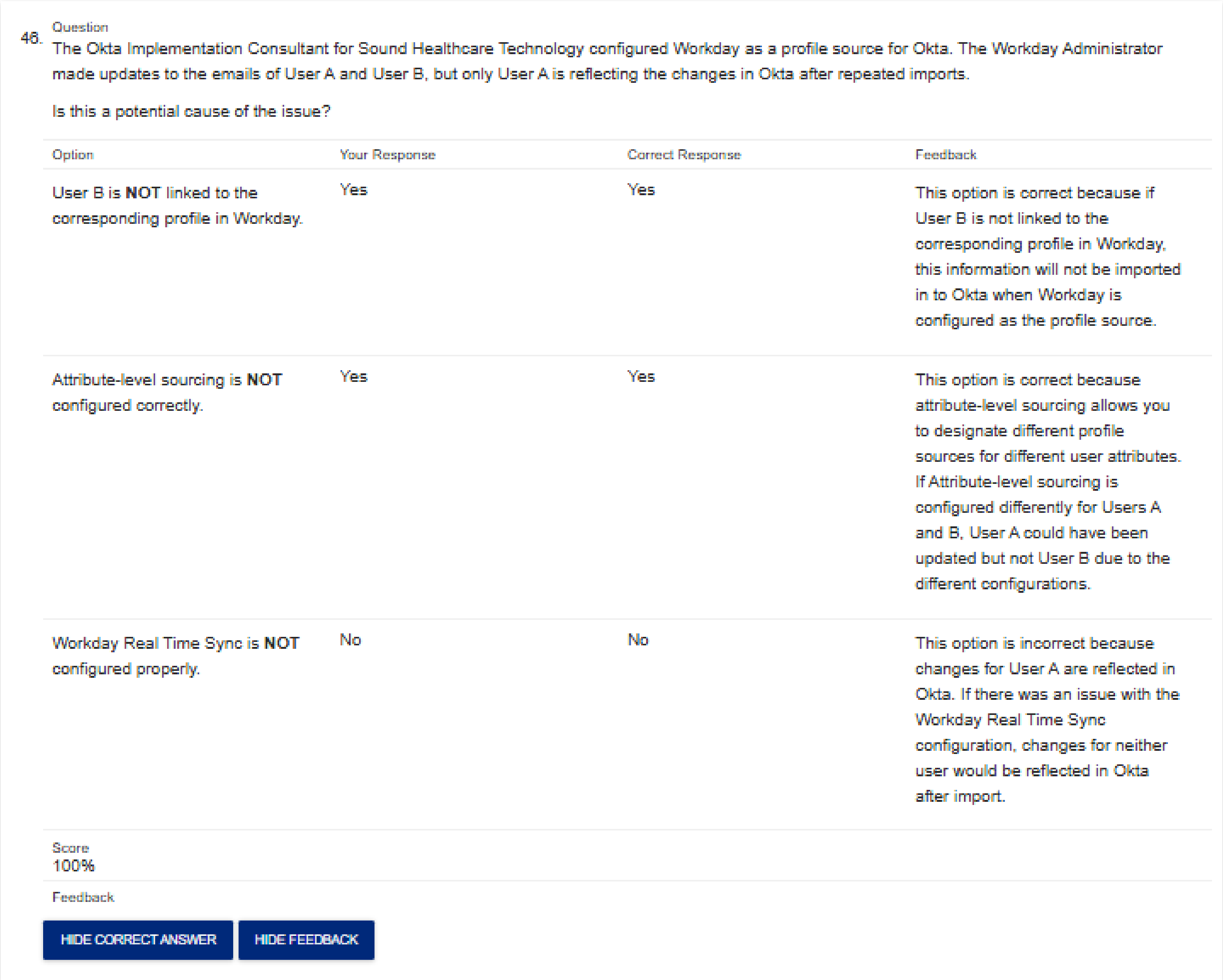
Sound Healthcare Technology wants to enforce Multifactor Authentication (MFA) for their employees who access the network remotely using a VPN. For technical reasons, the organization has multiple VPN solutions deployed on their infrastructure. Sound Healthcare Technology is unsure if a single Okta RADIUS server agent supports multiple integrations. The company has engaged an Okta Implementation Consultant to set up MFA with the Okta RADIUS server agent to support the integration with multiple RADIUS-enabled applications at the same time.

Is this a consideration the Okta Implementation Consultant must keep in mind when configuring MFA?

Option	Your Response	Correct Response	Feedback
A minimum of one Okta RADIUS server agent must be deployed for every RADIUS-enabled application.	No	No	This option is incorrect because one RADIUS app (not one Okta RADIUS server agent) must be added in Okta for each RADIUS-enabled application being integrated with Okta.
The Okta Implementation Consultant must change the config.properties file for the Okta RADIUS server agent and add one port number the agent will be listening to for each RADIUS-enabled application.	Yes	No	This option is incorrect because the Okta RADIUS server agent supports multiple ports simultaneously.

Score
0%

Feedback



46. Question

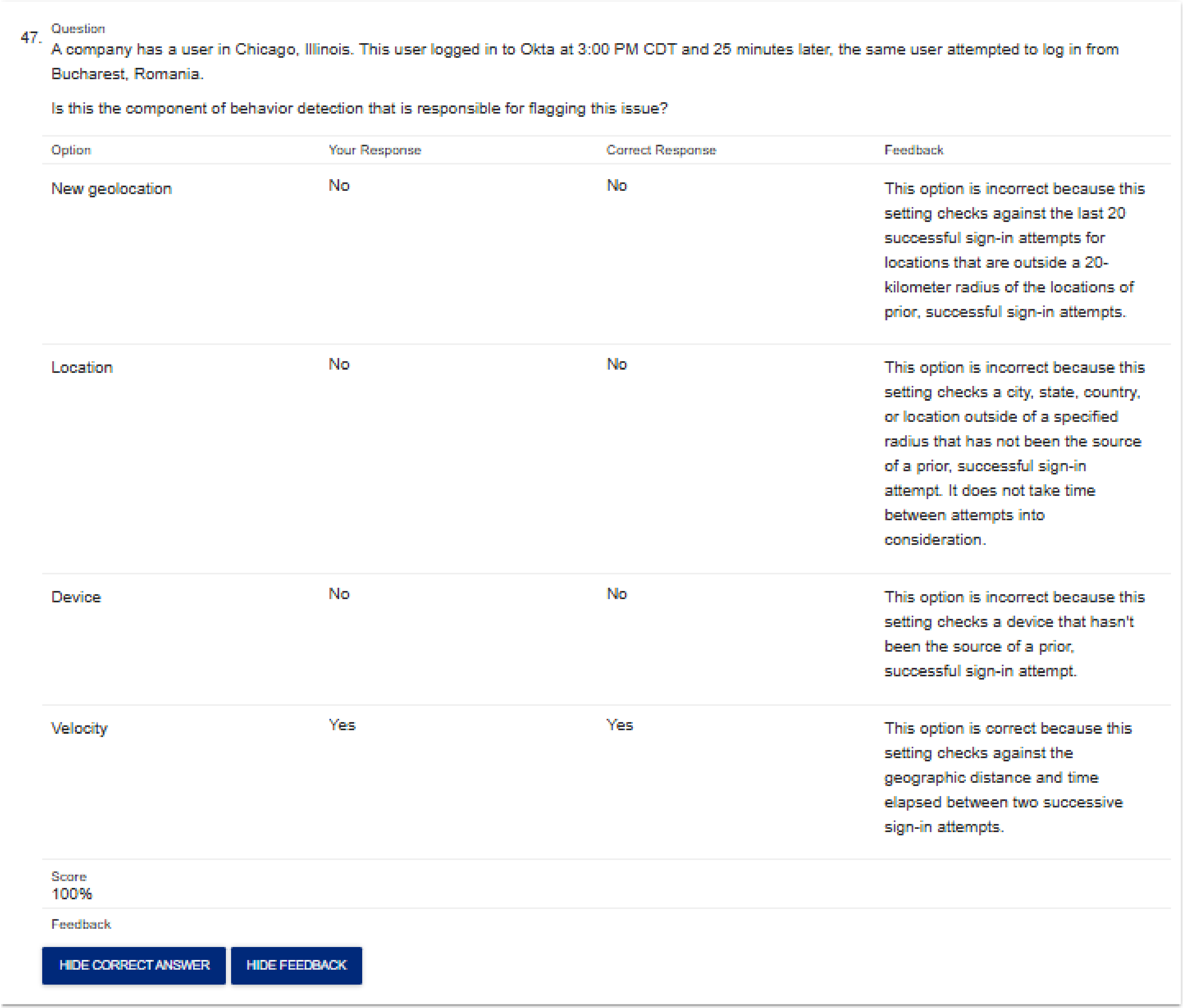
The Okta Implementation Consultant for Sound Healthcare Technology configured Workday as a profile source for Okta. The Workday Administrator made updates to the emails of User A and User B, but only User A is reflecting the changes in Okta after repeated imports.

Is this a potential cause of the issue?

Option	Your Response	Correct Response	Feedback
User B is **NOT** linked to the corresponding profile in Workday.	Yes	Yes	This option is correct because if User B is not linked to the corresponding profile in Workday, this information will not be imported in to Okta when Workday is configured as the profile source.
Attribute-level sourcing is **NOT** configured correctly.	Yes	Yes	This option is correct because attribute-level sourcing allows you to designate different profile sources for different user attributes. If Attribute-level sourcing is configured differently for Users A and B, User A could have been updated but not User B due to the different configurations.
Workday Real Time Sync is **NOT** configured properly.	No	No	This option is incorrect because changes for User A are reflected in Okta. If there was an issue with the Workday Real Time Sync configuration, changes for neither user would be reflected in Okta after import.

Score
100%

Feedback



47. Question

A company has a user in Chicago, Illinois. This user logged in to Okta at 3:00 PM CDT and 25 minutes later, the same user attempted to log in from Bucharest, Romania.

Is this the component of behavior detection that is responsible for flagging this issue?

Option	Your Response	Correct Response	Feedback
New geolocation	No	No	This option is incorrect because this setting checks against the last 20 successful sign-in attempts for locations that are outside a 20-kilometer radius of the locations of prior, successful sign-in attempts.
Location	No	No	This option is incorrect because this setting checks a city, state, country, or location outside of a specified radius that has not been the source of a prior, successful sign-in attempt. It does not take time between attempts into consideration.
Device	No	No	This option is incorrect because this setting checks a device that hasn't been the source of a prior, successful sign-in attempt.
Velocity	Yes	Yes	This option is correct because this setting checks against the geographic distance and time elapsed between two successive sign-in attempts.

Score
100%

Feedback