Question: 36 CertyIQ

HOTSPOT
-
You have a Microsoft 365 tenant that has 5,000 users. One hundred of the users are executives. The executives have a dedicated support team.
You need to ensure that the support team can reset passwords and manage multi-factor authentication (MFA) settings for only the executives. The solution must use the principle of least privilege.

Which object type and Azure Active Directory (Azure AD) role should you use? To answer, select the appropriate options in the answer area.
NOTE: Each correct selection is worth one point.

LIVEWORKSHEETS

Answer Area

Object type:

- An administrative unit
- A custom administrator role
- A dynamic group
- A Microsoft 365 group

Role:

- Authentication administrator
- Groups administrator
- Helpdesk administrator
- Password administrator

LIVEWORKSHEETS

Question: 42 CertyIQ

HOTSPOT
-
Your on-premises network contains an Active Directory domain that uses Azure AD Connect to sync with an Azure AD tenant.
You need to configure Azure AD Connect to meet the following requirements:

- User sign-ins to Azure AD must be authenticated by an Active Directory domain controller.
- Active Directory domain users must be able to use Azure AD self-service password reset (SSPR).

What should you use for each requirement? To answer, select the appropriate options in the answer area.
NOTE: Each correct selection is worth one point.

Answer Area

Authentication by the domain controller: [▼]
- Federation with Active Directory Federation Services (AD FS)
- Pass-through authentication
- Password hash synchronization

SSPR: [▼]
- Device writeback
- Group writeback
- Password hash synchronization
- Password writeback

LIVEWORKSHEETS

Question: 44 CertyIQ

Note: This question is part of a series of questions that present the same scenario. Each question in the series contains a unique solution that might meet the stated goals. Some question sets might have more than one correct solution, while others might not have a correct solution.
After you answer a question in this section, you will NOT be able to return to it. As a result, these questions will not appear in the review screen.
You have an Active Directory forest that syncs to an Azure AD tenant.
You discover that when a user account is disabled in Active Directory, the disabled user can still authenticate to Azure AD for up to 30 minutes.
You need to ensure that when a user account is disabled in Active Directory, the user account is immediately prevented from authenticating to Azure AD.
Solution: You configure conditional access policies.
Does this meet the goal?

A.Yes

B.No

LIVEWORKSHEETS

Question: 45 CertyIQ

Note: This question is part of a series of questions that present the same scenario. Each question in the series contains a unique solution that might meet the stated goals. Some question sets might have more than one correct solution, while others might not have a correct solution.
After you answer a question in this section, you will NOT be able to return to it. As a result, these questions will not appear in the review screen.
You have a Microsoft 365 E5 subscription.
You create a user named User1.
You need to ensure that User1 can update the status of Identity Secure Score improvement actions.
Solution: You assign the Exchange Administrator role to User1.
Does this meet the goal?

A. Yes

B. No

LIVEWORKSHEETS

Question: 46 CertyIQ

Note: This question is part of a series of questions that present the same scenario. Each question in the series contains a unique solution that might meet the stated goals. Some question sets might have more than one correct solution, while others might not have a correct solution.
After you answer a question in this section, you will NOT be able to return to it. As a result, these questions will not appear in the review screen.
You have a Microsoft 365 E5 subscription.
You create a user named User1.
You need to ensure that User1 can update the status of Identity Secure Score improvement actions.
Solution: You assign the User Administrator role to User1.
Does this meet the goal?

A. Yes

B. No

LIVEWORKSHEETS

Question: 47 CertyIQ

HOTSPOT
-
Case Study
-
Overview
-
Contoso, Ltd. is a consulting company that has a main office in Montreal and branch offices in London and Seattle.
Contoso has a partnership with a company named Fabrikam, Inc. Fabrikam has an Azure Active Directory (Azure AD) tenant named fabrikam.com.
Existing Environment. Existing Environment
The on-premises network of Contoso contains an Active Directory domain named contoso.com. The domain contains an organizational unit (OU) named Contoso_Resources. The Contoso_Resources OU contains all users and computers.
The contoso.com Active Directory domain contains the relevant users shown in the following table.

Name	Office	Department
Admin1	Montreal	Helpdesk
User1	Montreal	HR
User2	Montreal	HR
User3	Montreal	HR
Admin2	London	Helpdesk
User4	London	Finance
User5	London	Sales
User6	London	Sales
Admin3	Seattle	Helpdesk
User7	Seattle	Sales

LIVEWORKSHEETS

answer area.
NOTE: Each correct selection is worth one point.

Answer Area

Object to create for each branch office:

- An administrative unit
- A custom role
- A Dynamic User security group
- An OU

Tool to use:

- Azure Active Directory admin center
- Active Directory Administrative Center
- Active Directory module for Windows PowerShell
- Microsoft Purview Compliance porta

LIVEWORKSHEETS

Question: 48 CertyIQ

Case Study -
Overview -
ADatum Corporation is a consulting company in Montreal.
ADatum recently acquired a Vancouver-based company named Litware, Inc.
Existing Environment. ADatum Environment
The on-premises network of ADatum contains an Active Directory Domain Services (AD DS) forest named adatum.com.
ADatum has a Microsoft 365 E5 subscription. The subscription contains a verified domain that syncs with the adatum.com AD DS domain by using Azure AD Connect.
ADatum has an Azure Active Directory (Azure AD) tenant named adatum.com. The tenant has Security defaults disabled.
The tenant contains the users shown in the following table.

LIVEWORKSHEETS

•Users must provide one authentication method to reset their password by using SSPR. Available methods must include:
- Email
- Phone
- Security questions
- The Microsoft Authenticator app
•Trust relationships must NOT be established between the adatum.com and litware.com AD DS domains.
•The principle of least privilege must be used.

You need to resolve the issue of the sales department users.
What should you configure for the Azure AD tenant?

A.the Device settings

B.the User settings

C.the Access reviews settings

D.Security defaults

LIVEWORKSHEETS

Question: 49 CertyIQ

Case Study -
Overview -
ADatum Corporation is a consulting company in Montreal.
ADatum recently acquired a Vancouver-based company named Litware, Inc.
Existing Environment. ADatum Environment
The on-premises network of ADatum contains an Active Directory Domain Services (AD DS) forest named adatum.com.
ADatum has a Microsoft 365 E5 subscription. The subscription contains a verified domain that syncs with the adatum.com AD DS domain by using Azure AD Connect.
ADatum has an Azure Active Directory (Azure AD) tenant named adatum.com. The tenant has Security defaults disabled.
The tenant contains the users shown in the following table.

Name	Role
User1	*None*
User2	*None*
User3	User administrator
User4	Privileged role administrator
User5	Identity Governance Administrator

LIVEWORKSHEETS

- Email
- Phone
- Security questions
- The Microsoft Authenticator app

•Trust relationships must NOT be established between the adatum.com and litware.com AD DS domains.
•The principle of least privilege must be used.

You need to resolve the issue of IT_Group1.
What should you do first?

A.Change Membership type of IT_Group1 to Dynamic User.

B.Recreate the IT_Group1 group.

C.Change Membership type of IT Group1 to Dynamic Device.

D.Add an owner to IT_Group1.

LIVEWORKSHEETS

Question: 50 CertyIQ

Case Study -

Overview -
ADatum Corporation is a consulting company in Montreal.
ADatum recently acquired a Vancouver-based company named Litware, Inc.
Existing Environment. ADatum Environment
The on-premises network of ADatum contains an Active Directory Domain Services (AD DS) forest named adatum.com.
ADatum has a Microsoft 365 E5 subscription. The subscription contains a verified domain that syncs with the adatum.com AD DS domain by using Azure AD Connect.
ADatum has an Azure Active Directory (Azure AD) tenant named adatum.com. The tenant has Security defaults disabled.
The tenant contains the users shown in the following table.

Name	Role
User1	*None*
User2	*None*
User3	User administrator
User4	Privileged role administrator
[illegible]	[illegible]

LIVEWORKSHEETS

to one year.
•Users must be prompted to register for MFA and provided with an option to bypass the registration for a grace period.
•Users must provide one authentication method to reset their password by using SSPR. Available methods must include:
- Email
- Phone
- Security questions
- The Microsoft Authenticator app
•Trust relationships must NOT be established between the adatum.com and litware.com AD DS domains.
•The principle of least privilege must be used.
You need to implement the planned changes for litware.com.
What should you configure?

A.Azure AD Connect cloud sync between the Azure AD tenant and litware.com

B.Azure AD Connect to include the litware.com domain

C.staging mode in Azure AD Connect for the litware.com domain

LIVEWORKSHEETS

Question: 52 CertyIQ

HOTSPOT
-
You have an Azure AD tenant that contains a user named User1. User1 is assigned the User Administrator role.
You need to configure External collaboration settings for the tenant to meet the following requirements:
•Guest users must be prevented from querying staff email addresses.
•Guest users must be able to access the tenant only if they are invited by User1.
Which three settings should you configure? To answer, select the appropriate settings in the answer area.
NOTE: Each correct selection is worth one point.

LIVEWORKSHEETS