

Question: 442

CertyIQ

Introductory Info 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
User8	Seattle	Sales
User9	Seattle	Sales

Contoso also includes a marketing department that has users in each office.

Existing Environment. Microsoft 365/Azure Environment

Contoso has an Azure AD tenant named contoso.com that has the following associated licenses:

Microsoft Office 365 Enterprise E5

Enterprise Mobility + Security E5

Windows 10 Enterprise E3

Project Plan 3

Azure AD Connect is configured between Azure AD and Active Directory Domain Services (AD DS). Only the Contoso_Resources OU is synced.

Helpdesk administrators routinely use the Microsoft 365 admin center to manage user settings.

User administrators currently use the Microsoft 365 admin center to manually assign licenses. All users have all licenses assigned besides the following exceptions:

The users in the London office have the Microsoft 365 Phone System license unassigned.

The users in the Seattle office have the Yammer Enterprise license unassigned.

Security defaults are disabled for contoso.com.

Contoso uses Azure AD Privileged Identity Management (PIM) to protect administrative roles.

Existing Environment. Problem Statements

Contoso identifies the following issues:

Currently, all the helpdesk administrators can manage user licenses throughout the entire Microsoft 365 tenant.

The user administrators report that it is tedious to manually configure the different license requirements for each Contoso office.

Microsoft Office 365 Enterprise E5

Enterprise Mobility + Security E5

Windows 10 Enterprise E3

Project Plan 3

Azure AD Connect is configured between Azure AD and Active Directory Domain Services (AD DS). Only the Contoso_Resources OU is synced.

Helpdesk administrators routinely use the Microsoft 365 admin center to manage user settings.

User administrators currently use the Microsoft 365 admin center to manually assign licenses. All users have all licenses assigned besides the following exceptions:

The users in the London office have the Microsoft 365 Phone System license unassigned.

The users in the Seattle office have the Yammer Enterprise license unassigned.

Security defaults are disabled for contoso.com.

Contoso uses Azure AD Privileged Identity Management (PIM) to protect administrative roles.

Existing Environment. Problem Statements

Contoso identifies the following issues:

Currently, all the helpdesk administrators can manage user licenses throughout the entire Microsoft 365 tenant. The user administrators report that it is tedious to manually configure the different license requirements for each Contoso office.

The helpdesk administrators spend too much time provisioning internal and guest access to the required Microsoft 365 services and apps.

Currently, the helpdesk administrators can perform tasks by using the User administrator role without justification or approval.

When the Logs node is selected in Azure AD, an error message appears stating that Log Analytics integration is not enabled.

Requirements. Planned Changes -

Contoso plans to implement the following changes:

Implement self-service password reset (SSPR).

Analyze Azure audit activity logs by using Azure Monitor.

Simplify license allocation for new users added to the tenant.

Collaborate with the users at Fabrikam on a joint marketing campaign.

Configure the User administrator role to require justification and approval to activate.

Implement a custom line-of-business Azure web app named App1. App1 will be accessible from the internet and authenticated by using Azure AD accounts.

For new users in the marketing department, implement an automated approval workflow to provide access to a Microsoft SharePoint Online site, group, and app.

Contoso plans to acquire a company named ADatum Corporation. One hundred new ADatum users will be created in an Active Directory OU named Adatum. The users will be located in London and Seattle.

Requirements. Technical Requirements

Contoso identifies the following technical requirements:

All users must be synced from AD DS to the contoso.com Azure AD tenant.

App1 must have a redirect URI pointed to <https://contoso.com/auth-response>.

License allocation for new users must be assigned automatically based on the location of the user.

Fabrikam users must have access to the marketing department's SharePoint site for a maximum of 90 days. Administrative actions performed in Azure AD must be audited. Audit logs must be retained for one year. The helpdesk administrators must be able to manage licenses for only the users in their respective office. Users must be forced to change their password if there is a probability that the users' identity was compromised. Question You need to allocate licenses to the new users from ADatum. The solution must meet the technical requirements.

Which type of object should you create?

- A. a Dynamic User security group
- B. a distribution group
- C. an OU
- D. an administrative unit

Question: 443**CertyIQ**

Introductory Info 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
User8	Seattle	Sales
User9	Seattle	Sales

Contoso plans to implement the following changes:

Implement self-service password reset (SSPR).

Analyze Azure audit activity logs by using Azure Monitor.

Simplify license allocation for new users added to the tenant.

Collaborate with the users at Fabrikam on a joint marketing campaign.

Configure the User administrator role to require justification and approval to activate.

Implement a custom line-of-business Azure web app named App1. App1 will be accessible from the internet and authenticated by using Azure AD accounts.

For new users in the marketing department, implement an automated approval workflow to provide access to a Microsoft SharePoint Online site, group, and app.

Contoso plans to acquire a company named ADatum Corporation. One hundred new ADatum users will be created in an Active Directory OU named Adatum. The users will be located in London and Seattle.

Requirements. Technical Requirements

Contoso identifies the following technical requirements:

All users must be synced from AD DS to the contoso.com Azure AD tenant.

App1 must have a redirect URI pointed to <https://contoso.com/auth-response>.

License allocation for new users must be assigned automatically based on the location of the user.

Fabrikam users must have access to the marketing department's SharePoint site for a maximum of 90 days.

Administrative actions performed in Azure AD must be audited. Audit logs must be retained for one year.

The helpdesk administrators must be able to manage licenses for only the users in their respective office.

Users must be forced to change their password if there is a probability that the users' identity was compromised.

Question You need to sync the ADatum users. The solution must meet the technical requirements.

What should you do?

- A. From the Microsoft Azure Active Directory Connect wizard, select Customize synchronization options.
- B. From PowerShell, run Set-ADSyncScheduler.
- C. From PowerShell, run Start-ADSyncSyncCycle.
- D. From the Microsoft Azure Active Directory Connect wizard, select Change user sign-in.

Question: 444

Introductory Info 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
User8	Seattle	Sales
User9	Seattle	Sales

NOTE: Each correct selection is worth one point.

Hot Area:

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 365 admin center	

Question: 445

CertyIQ

Introductory Info 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.

Fabrikam users must have access to the marketing department's SharePoint site for a maximum of 90 days. Administrative actions performed in Azure AD must be audited. Audit logs must be retained for one year. The helpdesk administrators must be able to manage licenses for only the users in their respective office. Users must be forced to change their password if there is a probability that the users' identity was compromised. Question 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 Access reviews settings
- C. the User settings
- D. Security defaults

Question: 446

CertyIQ

Introductory Info Case Study -

Overview -

Litware, Inc. is a pharmaceutical company that has a subsidiary named Fabrikam, Inc.

Litware has offices in Boston and Seattle, but has employees located across the United States. Employees connect remotely to either office by using a VPN connection.

Existing Environment. Identity Environment

The network contains an Active Directory forest named litware.com that is linked to an Azure Active Directory (Azure AD) tenant named litware.com. Azure AD

Connect uses pass-through authentication and has password hash synchronization disabled.

Litware.com contains a user named User1 who oversees all application development.

Litware implements Azure AD Application Proxy.

Fabrikam has an Azure AD tenant named fabrikam.com. The users at Fabrikam access the resources in litware.com by using guest accounts in the litware.com tenant.

Existing Environment. Cloud Environment

All the users at Litware have Microsoft 365 Enterprise E5 licenses. All the built-in anomaly detection policies in

Answer Area

Azure AD Connect settings to modify:

	▼
Directory Extensions	
Domain Filtering	
Optional Features	

Assign Azure AD licenses to:

	▼
An Azure Active Directory group that has only nested groups	
An Azure Active Directory group that has the Assigned membership type	
An Azure Active Directory group that has the Dynamic User membership type	

Question: 447

CertyIQ

Introductory Info Case Study -

Overview -

Litware, Inc. is a pharmaceutical company that has a subsidiary named Fabrikam, Inc.

Litware has offices in Boston and Seattle, but has employees located across the United States. Employees connect remotely to either office by using a VPN connection.

Existing Environment. Identity Environment

The network contains an Active Directory forest named litware.com that is linked to an Azure Active Directory (Azure AD) tenant named litware.com. Azure AD

Connect uses pass-through authentication and has password hash synchronization disabled.

Litware.com contains a user named User1 who oversees all application development.

Litware implements Azure AD Application Proxy.

Fabrikam has an Azure AD tenant named fabrikam.com. The users at Fabrikam access the resources in litware.com by using guest accounts in the litware.com tenant.

Existing Environment. Cloud Environment

All the users at Litware have Microsoft 365 Enterprise E5 licenses. All the built-in anomaly detection policies in Microsoft Cloud App Security are enabled.

Litware has an Azure subscription associated to the litware.com Azure AD tenant. The subscription contains an Azure Sentinel instance that uses the Azure Active

Implement a banned password list for the litware.com forest.

Enforce MFA when accessing on-premises applications.

Automatically detect and remediate externally leaked credentials.

Requirements. Access Requirements

Litware identifies the following access requirements:

Control all access to all Azure resources and Azure AD applications by using conditional access policies.

Implement a conditional access policy that has session controls for Microsoft SharePoint Online.

Control privileged access to applications by using access reviews in Azure AD.

Requirements. Monitoring Requirements

Litware wants to use the Fusion rule in Azure Sentinel to detect multi-staged attacks that include a combination of suspicious Azure AD sign-ins followed by anomalous Microsoft Office 365 activity. Question You need to meet the authentication requirements for leaked credentials.

What should you do?

- A. Enable password hash synchronization in Azure AD Connect.
- B. Configure Azure AD Password Protection.
- C. Configure an authentication method policy in Azure AD.
- D. Enable federation with PingFederate in Azure AD Connect.

Question: 448

Introductory Info Case Study - Overview -

Litware, Inc. is a pharmaceutical company that has a subsidiary named Fabrikam, Inc. Litware has offices in Boston and Seattle, but has employees located across the United States. Employees connect remotely to either office by using a VPN connection.

Existing Environment. Identity Environment

The network contains an Active Directory forest named litware.com that is linked to an Azure Active Directory (Azure AD) tenant named litware.com. Azure AD

Connect uses pass-through authentication and has password hash synchronization disabled.

Litware.com contains a user named User1 who oversees all application development.

Litware implements Azure AD Application Proxy.

Fabrikam has an Azure AD tenant named fabrikam.com. The users at Fabrikam access the resources in litware.com by using guest accounts in the litware.com tenant.

Existing Environment. Cloud Environment

All the users at Litware have Microsoft 365 Enterprise E5 licenses. All the built-in anomaly detection policies in Microsoft Cloud App Security are enabled.

Litware has an Azure subscription associated to the litware.com Azure AD tenant. The subscription contains an Azure Sentinel instance that uses the Azure Active

Directory connector and the Office 365 connector. Azure Sentinel currently collects the Azure AD sign-ins logs and audit logs.

Existing Environment. On-premises Environment

The on-premises network contains the servers shown in the following table.

Name	Operating system	Office	Description
DC1	Windows Server 2019	Boston	Domain controller for litware.com
SERVER1	Windows Server 2019	Boston	Member server in litware.com that runs the Azure AD Application Proxy connector
SERVER2	Windows Server 2019	Boston	Member server that uses Azure AD Connect