

### Question: 450

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.

Question HOTSPOT -

You need to meet the technical requirements for the probability that user identities were compromised.

What should the users do first, and what should you configure? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Hot Area:

**Answer Area**

The users must first:

|                                                            |   |
|------------------------------------------------------------|---|
|                                                            | ▼ |
| Provide consent for any app to access the data of Contoso. |   |
| Register for multi-factor authentication (MFA).            |   |
| Register for self-service password reset (SSPR).           |   |

You must configure:

|                                        |   |
|----------------------------------------|---|
|                                        | ▼ |
| A sign-in risk policy                  |   |
| A user risk policy                     |   |
| An Azure AD Password Protection policy |   |

Question: 451

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

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                                        |

Both Litware offices connect directly to the internet. Both offices connect to virtual networks in the Azure subscription by using a site-to-site VPN connection. All on-premises domain controllers are prevented from accessing the internet.

### Requirements. Delegation Requirements

Litware identifies the following delegation requirements:

Delegate the management of privileged roles by using Azure AD Privileged Identity Management (PIM).

Prevent nonprivileged users from registering applications in the litware.com Azure AD tenant.

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 configure the MFA settings for users who connect from the Boston office. The solution must meet the authentication requirements and the access requirements.

What should you include in the configuration?

- A. named locations that have a private IP address range
- B. named locations that have a public IP address range
- C. trusted IPs that have a public IP address range
- D. trusted IPs that have a private IP address range

## Question: 452

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

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.

## Answer Area

Feature:

|                                                 |   |
|-------------------------------------------------|---|
|                                                 | ▼ |
| An authentication method policy                 |   |
| A Conditional Access policy                     |   |
| An MFA registration policy                      |   |
| The Multi-Factor Authentication Server settings |   |

Grace period:

|         |   |
|---------|---|
|         | ▼ |
| 7 days  |   |
| 14 days |   |
| 28 days |   |

**Question: 453****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 Planner 2

Marketing users must have access to the marketing department's intranet site for a maximum of 30 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 meet the planned changes and technical requirements for App1.  
What should you implement?

- A. a policy set in Microsoft Endpoint Manager
- B. an app configuration policy in Microsoft Endpoint Manager
- C. an app registration in Azure AD
- D. Azure AD Application Proxy

### Question: 454

#### 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                                        |

Both Litware offices connect directly to the internet. Both offices connect to virtual networks in the Azure subscription by using a site-to-site VPN connection. All on-premises domain controllers are prevented from accessing the internet.

#### Requirements. Delegation Requirements

suspicious Azure AD sign-ins followed by anomalous Microsoft Office 365 activity. Question HOTSPOT - You need to implement on-premises application and SharePoint Online restrictions to meet the authentication requirements and the access requirements. What should you do? To answer, select the appropriate options in the answer area. NOTE: Each correct selection is worth one point. Hot Area:

Answer Area

For on-premises applications:

▼

Configure Cloud App Security policies.

Modify the User consent settings for the enterprise applications.

Publish the applications by using Azure AD Application Proxy.

For SharePoint Online:

▼

Configure app-enforced restrictions.

Modify the User consent settings for the enterprise applications.

Publish an application by using Azure AD Application Proxy.

### Question: 455

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

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                                        |

Both Litware offices connect directly to the internet. Both offices connect to virtual networks in the Azure

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 HOTSPOT - You need to configure app registration in Azure AD to meet the delegation requirements.

What should you do? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Hot Area:

## Answer Area

Azure AD tenant-level setting to modify:

|                                                                       |   |
|-----------------------------------------------------------------------|---|
|                                                                       | ▼ |
| Allow users to register application                                   |   |
| Users can consent to apps accessing company data on their behalf      |   |
| Users can request admin consent to apps they are unable to consent to |   |

Role to assign to User1:

|                                 |   |
|---------------------------------|---|
|                                 | ▼ |
| Application administrator       |   |
| Application developer           |   |
| Cloud application administrator |   |

**Question: 456****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                                        |