Set the frequency to:

One time	V
Weekly	
Monthly	

To ensure that access is removed if an administrator fails to respond, configure the:

Upon completion settings	V
Advanced settings	
Programs	
Reviewers	

QUESTION 8
HOTSPOT
You install Azure ATP sensors on domain controllers.

You add a member to the Domain Admins group. You view the timeline in Azure ATP and discover that information regarding the membership change is missing.

You need to meet the security requirements for Azure ATP reporting.

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

NOTE: Each correct selection is worth one point.

Policy to edit:

Default Domain Controllers Policy
Default Domain Policy
A local policy on one domain controller

Audit setting to configure:

Audit User Account Management
Audit Computer Account Management
Audit Other Account Management Events
Audit Security Group Management

Correct Answer:

Policy to edit: ▼

| Default Domain Controllers Policy |
| Default Domain Policy |
| A local policy on one domain controller |

Audit setting to configure: ▼

| Audit User Account Management |
| Audit Computer Account Management |
| Audit Other Account Management Events |
| Audit Security Group Management |

Topic 2, Litware, Inc

Overview

Litware, Inc. is a financial company that has 1,000 users in its main office in Chicago and 100 users in a branch office in San Francisco.

Existing Environment
Internal Network Infrastructure

The network contains a single domain forest. The forest functional level is Windows Server 2016.

Users are subject to sign-in hour restrictions as defined in Active Directory.

The network has the IP address range shown in the following table.

Location	IP address range
Chicago office internal network	192.168.0.0/20
Chicago office perimeter network	172.16.0.0/24
Chicago office external network	131.107.83.0/28
San Francisco office internal network	192.168.16.0/20
San Francisco office perimeter network	172.16.16.0/24
San Francisco office external network	131.107.16.218/32

The offices connect by using Multiprotocol Label Switching (MPLS).

The following operating systems are used on the network:

- Windows Server 2016
- Windows 10 Enterprise
- Windows 8.1 Enterprise

The internal network contains the systems shown in the following table.

Office	Name	Configuration
Chicago	DC1	Domain controller
Chicago	DC2	Domain controller
San Francisco	DC3	Domain controller
Chicago	Server1	SIEM-server

Litware uses a third-party email system.

Cloud Infrastructure
Litware recently purchased Microsoft 365 subscription licenses for all users.

Microsoft Azure Active Directory (Azure AD) Connect is installed and uses the default authentication settings. User accounts are not yet synced to Azure AD.

You have the Microsoft 365 users and groups shown in the following table.

Name	Object type	Description
Group 1	Security group	A group for testing Azure and Microsoft 365 functionality
User1	User	A test user who is a member of Group1
User2	User	A test user who is a member of Group1
User3	User	A test user who is a member of Group1
User4	User	An administrator
Guest1	Guest user	A guest user

Planned Changes
Litware plans to implement the following changes:

 ▪ Migrate the email system to Microsoft Exchange Online
 ▪ Implement Azure AD Privileged Identity Management

Security Requirements
Litware identities the following security requirements:

 ▪ Create a group named Group2 that will include all the Azure AD user accounts. Group2 will be used to provide limited access to Windows Analytics
 ▪ Create a group named Group3 that will be used to apply Azure Information Protection policies to pilot users. Group3 must only contain user accounts
 ▪ Use Azure Advanced Threat Protection (ATP) to detect any security threats that target the forest
 ▪ Prevent users locked out of Active Directory from signing in to Azure AD and Active Directory
 ▪ Implement a permanent eligible assignment of the Compliance administrator role for User1
 ▪ Integrate Windows Defender and Windows Defender ATP on domain-joined servers
 ▪ Prevent access to Azure resources for the guest user accounts by default
 ▪ Ensure that all domain-joined computers are registered to Azure AD

Multi-factor authentication (MFA) Requirements
Security features of Microsoft Office 365 and Azure will be tested by using pilot Azure user accounts.

You identify the following requirements for testing MFA:

▪ Pilot users must use MFA unless they are signing in from the internal network of the Chicago office. MFA must NOT be used on the Chicago office internal network.
▪ If an authentication attempt is suspicious, MFA must be used, regardless of the user location.
▪ Any disruption of legitimate authentication attempts must be minimized.

General Requirements
Litware want to minimize the deployment of additional servers and services in the Active Directory forest.

QUESTION 1
HOTSPOT
How should you configure Group3? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Group type:

| An Office 365 group in the Microsoft 365 admin center |
| A security group in Active Directory Users and Computers |
| A security group in the Azure Active Directory admin center |

Group membership criteria:

| A dynamic distribution list |
| A dynamic membership rule with an Advanced rule set to All users |
| A dynamic membership rule with a Simple rule set to userType Equals User |

Correct Answer:

Group type:

| An Office 365 group in the Microsoft 365 admin center |
| A security group in Active Directory Users and Computers |
| A security group in the Azure Active Directory admin center |

Group membership criteria:

| A dynamic distribution list |
| A dynamic membership rule with an Advanced rule set to All users |
| A dynamic membership rule with a Simple rule set to userType Equals User |

QUESTION 2
You need to implement Windows Defender ATP to meet the security requirements. What should you do?

A.   Configure port mirroring
B.   Create the ForceDefenderPassiveMode registry setting
C.   Download and install the Microsoft Monitoring Agent
D.   Run WindowsDefenderATPOnboardingScript.cmd

Correct Answer: C

QUESTION 3
Which IP address space should you include in the MFA configuration?

A.   131.107.83.0/28
B.   192.168.16.0/20
C.   172.16.0.0/24
D.   192.168.0.0/20

Correct Answer: B

QUESTION 4
You need to create Group2. What are two possible ways to create the group?

A.   an Office 365 group in the Microsoft 365 admin center
B.   a mail-enabled security group in the Microsoft 365 admin center
C.   a security group in the Microsoft 365 admin center
D.   a distribution list in the Microsoft 365 admin center
E.   a security group in the Azure AD admin center

Correct Answer: CE

QUESTION 5
You need to create Group3. What are two possible ways to create the group?

A.   an Office 365 group in the Microsoft 365 admin center
B.   a mail-enabled security group in the Microsoft 365 admin center
C.   a security group in the Microsoft 365 admin center
D.   a distribution list in the Microsoft 365 admin center
E.   a security group in the Azure AD admin center

Correct Answer: AD