11/02/2025

CLOUD SECURITY REPORT
TEAM 4

Table of Contents

List of Tables

List of Figures

Executive Summary

As CyberBulwork transitions its infrastructure to the cloud, it has been a priority to ensure robust security, compliance, and seamless identity management. This report outlines the deployment of key security solutions, including Microsoft Sentinel for threat detection, Microsoft Purview DLP for data loss prevention, and Azure AD DS for identity synchronization, to enhance cybersecurity and operational efficiency.

The implementation of Microsoft Sentinel provided advanced threat intelligence and real-time monitoring capabilities, allowing for proactive security incident management. Microsoft Purview DLP was configured to prevent unauthorized data transfers, ensuring compliance with organizational policies and regulatory requirements. Additionally, Azure AD DS was deployed to extend on-premises Active Directory to the cloud, enabling secure and seamless access to resources for employees.

During the deployment, challenges such as fine-tuning Sentinel to reduce false positives, troubleshooting DLP policies for effective detection, and resolving synchronization issues in Azure AD DS were encountered. However, through systematic troubleshooting and iterative improvements, these challenges were successfully addressed.

The result is a more secure, resilient, and compliant cloud infrastructure for CyberBulwork, with improved threat detection, data protection, and identity management. These enhancements position the organization to effectively mitigate risks, safeguard sensitive information, and ensure a seamless transition to cloud-based operations.

Identity and Access Management - Azure Active Directory

1.1 Introduction

Cyberbulwork's management has decided to migrate its on-prem infrastructure to the cloud as part of a strategic digital transformation. Our team has been assigned the responsibility of executing this migration and providing a comprehensive report on the process. To ensure a secure transition, we are implementing identity and access management controls to regulate user permissions and protect cloud resources.

As part of this migration, each staff member of Cyberbulwork needs to be assigned the appropriate level of access required for their role while maintaining security best practices. Additionally, we must establish a logging and monitoring system to track access events and enforce compliance policies.

To achieve seamless identity management, we leveraged Active Directory Domain Services (AD DS) in conjunction with Azure Active Directory (AAD) to synchronize on-prem identities with the cloud. This hybrid approach ensures a smooth transition while maintaining centralized control over user authentication and access management

1.2 Users and Roles

Table 1 provides an overview of Cyberbulwork's team members, their respective roles, and the level of access granted to them based on their responsibilities. Assigning appropriate access permissions ensures that each user has the necessary privileges to perform their tasks securely while maintaining strict control over sensitive resources.

Table 1: User Roles and Access Requirements

S/N	User	Role	Access Required
1	Etinosa Imafidon	Chief Information Officer	Global Reader, Compliance Administrator, Global Administrator, Global Secure Access Administrator.
2	Motunrayo Sanusi	Cybersecurity Engineer	Security Admin, Attribute Log Admin
3	Daniel Owoeye-Wise	System Administrator	Privileged Role Admin, Password Admin
4	Shado Peculiar Unini	Human Resource Manager	Privileged Role Administrator, User Admin

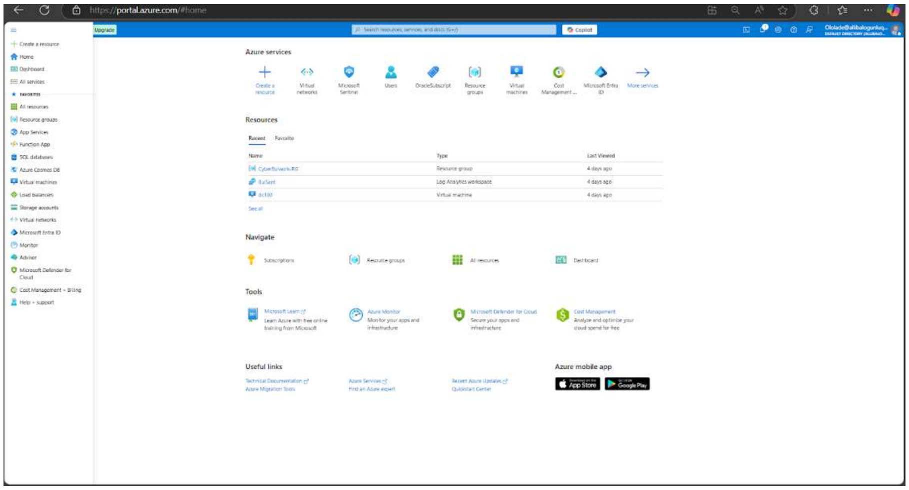
5	Alli-Balogun Luqman Damilare	Intern	Limited User Access
6	Ololade Elizabeth Adesagba	Head of Finance	Global Reader, Report Reader
7	Oluwaseyi Adebayo	Database Administrator	Authentication Admin, Cloud Device Admin
8	Muizz Babatunde Majeed	Software Engineer	App Admin, App Developer, Cloud App Admin
9	Dike Promise Chimamanda	Customer Service Officer	Basic User Access

1.3 Creation of Azure Account

To facilitate Cyberbulwork’s migration to the cloud, an Azure account was created for the organization through the Azure portal. The setup process followed the standard registration prompts on the Azure website, ensuring that all necessary configurations were in place for a smooth deployment. **Figure 1** provides a snapshot of the newly created account.

1.4 Cost Management

Following the account setup, cost management was configured to monitor and control Cyberbulwork’s Azure credit spending. This implementation ensures that the organization can track resource usage, set budget limits, and optimize cloud expenses effectively. **Figure 1.2** displays the cost management setup.



Name	Type	Last Viewed
CyberBulwork-RG	Resource group	4 days ago
BulSent	Log Analytics workspace	4 days ago
dc100	Virtual machine	4 days ago

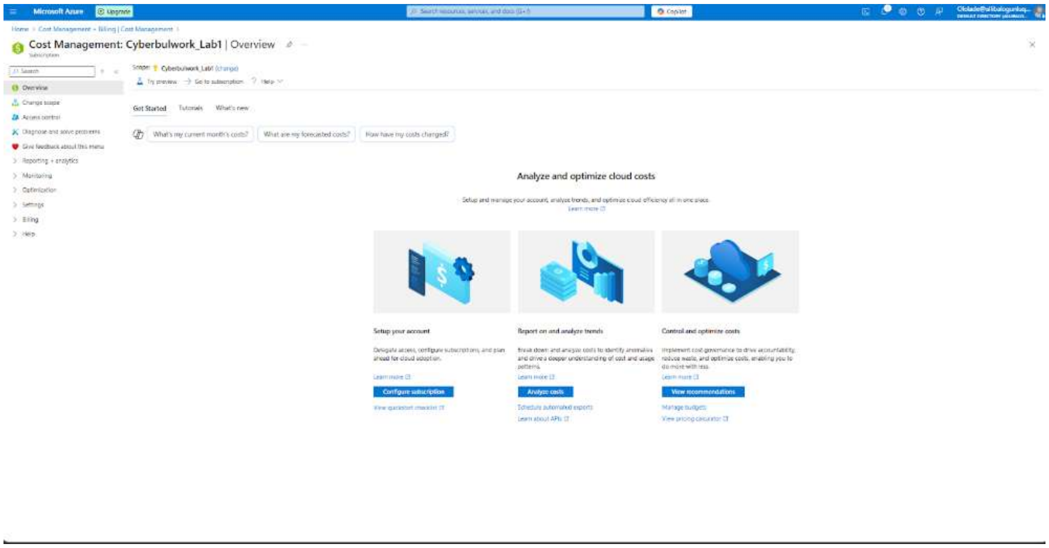
Learn Azure with free online training from Microsoft

Monitor your apps and infrastructure

Secure your apps and infrastructure

Analyze and optimize your cloud spend for free

Figure 1: Azure account creation


Microsoft Azure
Upgrade
Search resources, services, and docs (G+/)
Copilot
Ololade@allibalogunluq...
DEFAULT DIRECTORY
Home > Cost Management + Billing | Cost Management >
Cost Management: Cyberbulwork_Lab1 | Overview
Subscription
Search
Overview
Change scope
Access control
Diagnose and solve problems
Give feedback about this menu
Reporting + analytics
Monitoring
Optimization
Settings
Billing
Help
Scope: Cyberbulwork_Lab1 (change)
Try preview
Go to subscription
Help
Get Started
Tutorials
What's new
What's my current month's costs?
What are my forecasted costs?
How have my costs changed?
Analyze and optimize cloud costs
Learn more
Setup your account
Report on and analyze trends
Control and optimize costs
Learn more
Configure subscription
View quickstart checklist
Analyze costs
Schedule automated exports
Learn about APIs
View recommendations
Manage budgets
View pricing calculator

Setup and manage your account, analyze trends, and optimize cloud efficiency all in one place.

Delegate access, configure subscriptions, and plan ahead for cloud adoption.

Break down and analyze costs to identify anomalies and drive a deeper understanding of cost and usage patterns.

Implement cost governance to drive accountability, reduce waste, and optimize costs, enabling you to do more with less.

Figure 2: Cost Management creation

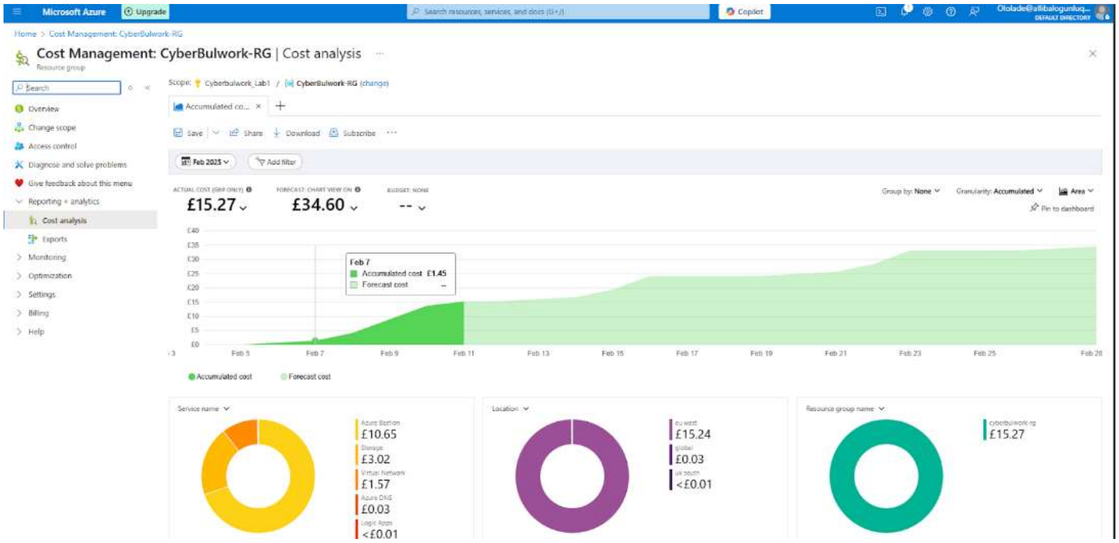


Figure 3: Cost Management Analysis

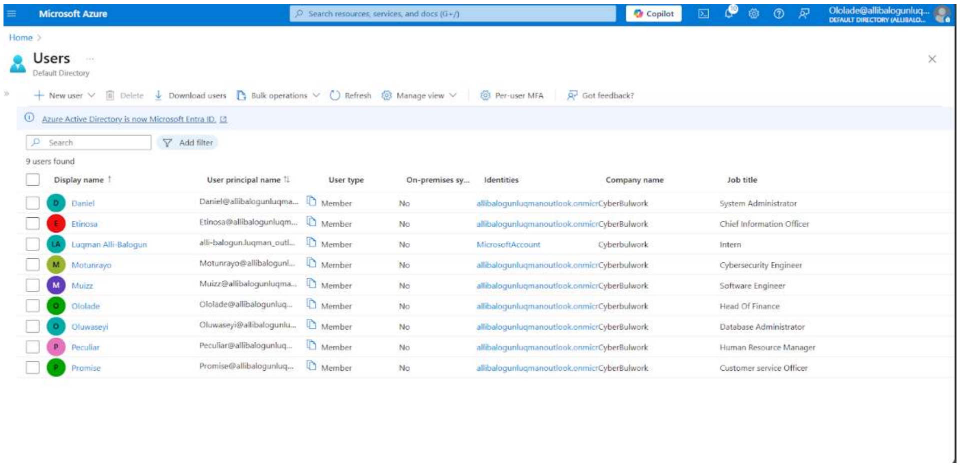
1.5 Identity and Access Management

The team was tasked with implementing Identity and Access Management (IAM) on Azure Active Directory (AAD) to ensure secure user authentication and authorization. This process involved:

- Setting up users based on their designated roles within the organization.
- Implementing Role-Based Access Control (RBAC) to assign permissions appropriately.
- Configuring Multi-Factor Authentication (MFA) to enhance security.
- Enforcing MFA for all users to mitigate unauthorized access risks.

1.6 User Setup Based on Roles

Users were successfully created and configured within Azure IAM according to their specific roles in Cyberbulwork. This structured approach ensures that each user has the necessary permissions aligned with their responsibilities while maintaining strict security controls.



Azure Active Directory is now Microsoft Entra ID.

Search

Add filter

9 users found

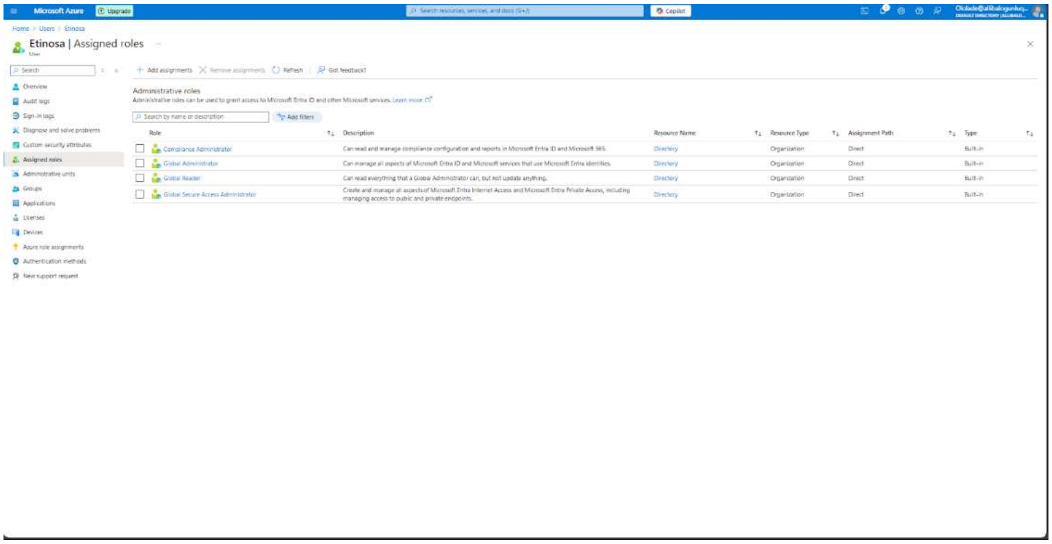
Display name	User principal name	User type	On-premises sy...	Identities	Company name	Job title
Daniel	Daniel@allibalogunluqma...	Member	No	allibalogunluqmanoutlook.onmicr	CyberBulwork	System Administrator
Etinosa	Etinosa@allibalogunluqm...	Member	No	allibalogunluqmanoutlook.onmicr	CyberBulwork	Chief Information Officer
Luqman Alli-Balogun	alli-balogun.luqman_outl...	Member	No	MicrosoftAccount	Cyberbulwork	Intern
Motunrayo	Motunrayo@allibalogunl...	Member	No	allibalogunluqmanoutlook.onmicr	Cyberbulwork	Cybersecurity Engineer
Muizz	Muizz@allibalogunluqma...	Member	No	allibalogunluqmanoutlook.onmicr	CyberBulwork	Software Engineer
Ololade	Ololade@allibalogunluq...	Member	No	allibalogunluqmanoutlook.onmicr	Cyberbulwork	Head Of Finance
Oluwaseyi	Oluwaseyi@allibalogunlu...	Member	No	allibalogunluqmanoutlook.onmicr	CyberBulwork	Database Administrator
Peculiar	Peculiar@allibalogunluq...	Member	No	allibalogunluqmanoutlook.onmicr	CyberBulwork	Human Resource Manager
Promise	Promise@allibalogunluq...	Member	No	allibalogunluqmanoutlook.onmicr	CyberBulwork	Customer service Officer

Figure 4: List of Created Users on Entra ID

1.7 RBAC Implementation for Users

Role-Based Access Control (RBAC) was successfully implemented for all user accounts created in Azure Active Directory. This ensures that users have only the necessary permissions required for their roles, reinforcing the principle of least privilege and maintaining a structured, secure access management system.

By aligning access levels with job responsibilities, Cyberbulwork enhances security, minimizes unauthorized access risks, and ensures compliance with industry best practices. Figure 1.4 illustrates an example of RBAC implementation for the Chief Information Officer (CIO), showcasing the specific permissions assigned to this role.



Administrative roles

Administrative roles can be used to grant access to Microsoft Entra ID and other Microsoft services. Learn more

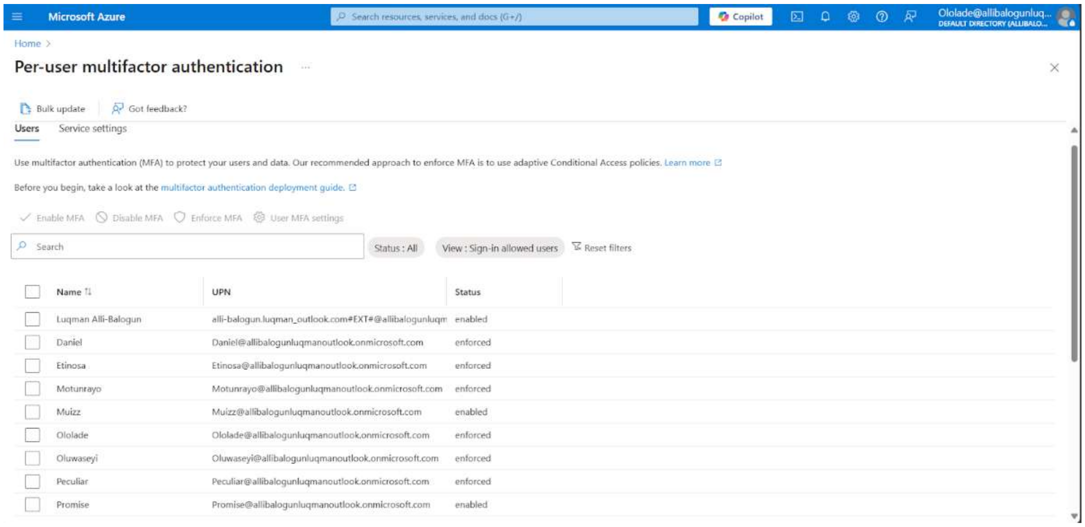
Role	Description	Resource Name	Resource Type	Assignment Path	Type
Compliance Administrator	Can read and manage compliance configuration and reports in Microsoft Entra ID and Microsoft 365.	Directory	Organization	Direct	Built-in
Global Administrator	Can manage all aspects of Microsoft Entra ID and Microsoft services that use Microsoft Entra identities.	Directory	Organization	Direct	Built-in
Global Reader	Can read everything that a Global Administrator can, but not update anything.	Directory	Organization	Direct	Built-in
Global Secure Access Administrator	Create and manage all aspectsof Microsoft Entra Internet Access and Microsoft Entra Private Access, including managing access to public and private endpoints.	Directory	Organization	Direct	Built-in

Figure 5: RBAC implementation for the Chief Information Officer (CIO)

1.8 MFA Configuration

Multi-factor authentication (MFA) was successfully configured and enforced for all user accounts created on the Azure platform. This additional layer of security strengthens user authentication by requiring a second verification step beyond passwords, reducing the risk of unauthorized access and potential security breaches.

To streamline the authentication process, Microsoft Authenticator was designated as the second-level authentication method for all users. Figure 1.5 below illustrates the MFA setup and configuration.


Microsoft Azure
Search resources, services, and docs (G+/)
Copilot
Ololade@allibalogunluq...
DEFAULT DIRECTORY (ALLIBALO...
Home >

Per-user multifactor authentication

Use multifactor authentication (MFA) to protect your users and data. Our recommended approach to enforce MFA is to use adaptive Conditional Access policies. Learn more

Before you begin, take a look at the multifactor authentication deployment guide.

Name	UPN	Status
Luqman Alli-Balogun	alli-balogun.luqman_outlook.com#EXT#@allibalogunluqm	enabled
Daniel	Daniel@allibalogunluqmanoutlook.onmicrosoft.com	enforced
Etinosa	Etinosa@allibalogunluqmanoutlook.onmicrosoft.com	enforced
Motunrayo	Motunrayo@allibalogunluqmanoutlook.onmicrosoft.com	enforced
Muizz	Muizz@allibalogunluqmanoutlook.onmicrosoft.com	enabled
Ololade	Ololade@allibalogunluqmanoutlook.onmicrosoft.com	enforced
Oluwaseyi	Oluwaseyi@allibalogunluqmanoutlook.onmicrosoft.com	enforced
Peculiar	Peculiar@allibalogunluqmanoutlook.onmicrosoft.com	enforced
Promise	Promise@allibalogunluqmanoutlook.onmicrosoft.com	enabled

Figure 6: MFA Activation for all Users

1.9 Challenges Encountered

1. Identification of Directory Roles

The team faced challenges in identifying the correct directory roles for users. Without a clear understanding of each role's permissions, assigning appropriate access was difficult. To address this, we conducted extensive research, reviewed Azure documentation, and referenced Microsoft's official resources. This highlights the need for thorough documentation review to ensure a well-structured Identity and Access Management (IAM) system.

2. User Provisioning and Synchronization Issues

During the integration of Azure Active Directory (AAD) with on-premises Active Directory, we encountered user provisioning and synchronization issues. Some accounts failed to sync properly, causing delays in granting access. The team resolved this by verifying synchronization settings, ensuring that directory services were correctly configured, and troubleshooting manual sync failures when necessary.

3. User Login Issues Post-MFA Enablement

After MFA enforcement, several users experienced login issues, which caused temporary access disruptions. The challenges ranged from incorrect MFA setup to authentication failures. The team provided step-by-step guidance to affected users and ensured that authentication settings were correctly configured, reinforcing the importance of proactive user support and troubleshooting during security implementations.

4. Audit, Monitoring and Logging on Cloud - Audit Logs/Azure Sentinel.

After assigning roles and access to users, a robust monitoring and analysis platform was essential to track user activity, endpoint health, and application performance. To fulfill this need, Azure Sentinel, a Security Information and Event Management (SIEM) solution, was deployed.

By leveraging Azure Audit Logs and Sentinel's advanced analytics, the system enhances compliance, detects security threats, facilitates incident response, and monitors role-based access control (RBAC) activity. This implementation provides deep visibility into user interactions, strengthens threat detection and response, and supports ongoing compliance efforts within the Azure environment.

Creating and Deploying the Virtual Machine

A Virtual Machine (VM) was deployed to serve as a monitored endpoint in Azure Sentinel. The machine was assigned to the "IT" resource group and configured with the following specifications:

- Operating System: Windows Server 2019 Datacenter
- Size: Standard_B1s – 1 vCPU, 1 GB memory

Figures 2.1 to 2.3 illustrate the virtual machine creation process.

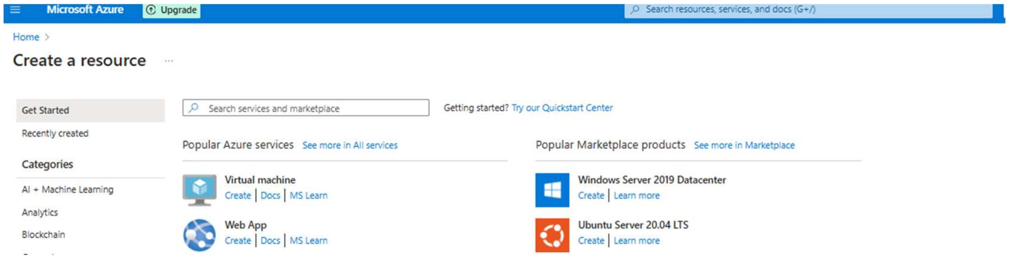
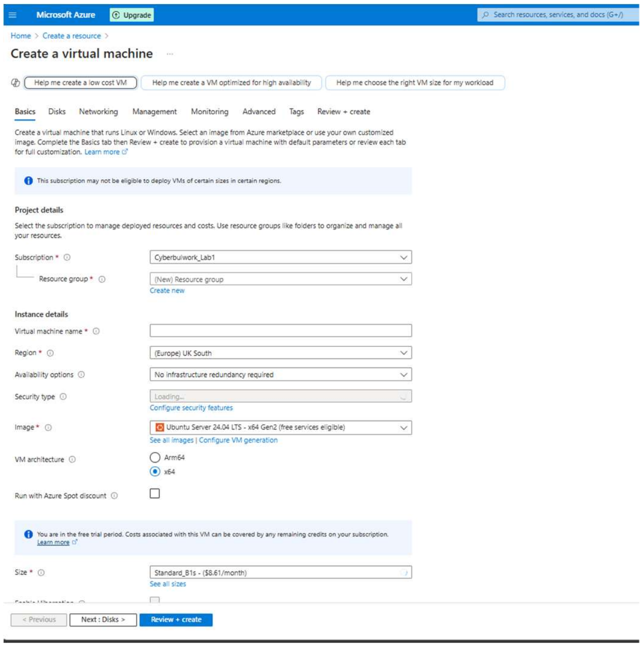


Figure 7: Creating the Resource



Microsoft Azure
Upgrade
Search resources, services, and docs (G+/)
Home > Create a resource >
Help me create a low cost VM
Help me create a VM optimized for high availability
Help me choose the right VM size for my workload
Basics
Disks
Networking
Management
Monitoring
Advanced
Tags
Review + create
< Previous
Next : Disks >
Review + create

Create a virtual machine

Create a virtual machine that runs Linux or Windows. Select an image from Azure marketplace or use your own customized image. Complete the Basics tab then Review + create to provision a virtual machine with default parameters or review each tab for full customization. Learn more

This subscription may not be eligible to deploy VMs of certain sizes in certain regions.

Project details

Select the subscription to manage deployed resources and costs. Use resource groups like folders to organize and manage all your resources.

Subscription * : Cyberbulwork_Lab1

Resource group * : (New) Resource group

Create new

Instance details

Virtual machine name * :

Region * : (Europe) UK South

Availability options : No infrastructure redundancy required

Security type : Loading...

Configure security features

Image * : Ubuntu Server 24.04 LTS - x64 Gen2 (free services eligible)

See all images | Configure VM generation

VM architecture : ○ Arm64 ● x64

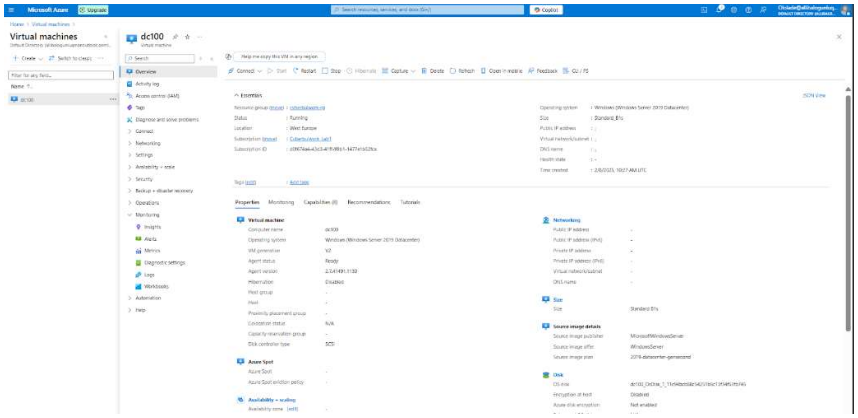
Run with Azure Spot discount : □

You are in the free trial period. Costs associated with this VM can be covered by any remaining credits on your subscription. Learn more

Size * : Standard_B1s - ($8.61/month)

See all sizes

Figure 8: Selecting Configuration Settings



dc100

Virtual machine

Essentials

Status : Running

Location : West Europe

Subscription (move) : Cyberbulwork_Lab1

Operating system : Windows (Windows Server 2019 Datacenter)

Size : Standard_B1s

Virtual machine

Computer name : dc100

Operating system : Windows (Windows Server 2019 Datacenter)

VM generation : V2

Agent status : Ready

Agent version : 2.7.41491.1139

Hibernation : Disabled

Host group : -

Host : -

Proximity placement group : -

Colocation status : N/A

Capacity reservation group : -

Disk controller type : SCSI

Azure Spot

Azure Spot : -

Azure Spot eviction policy : -

Availability + scaling

Availability zone (edit) : -

Networking

Public IP address : -

Public IP address (IPv6) : -

Private IP address : -

Private IP address (IPv6) : -

Virtual network/subnet : -

DNS name : -

Size

Size : Standard B1s

Source image details

Source image publisher : MicrosoftWindowsServer

Source image offer : WindowsServer

Source image plan : 2019-datacenter-gensecond

Disk

Encryption at host : Disabled

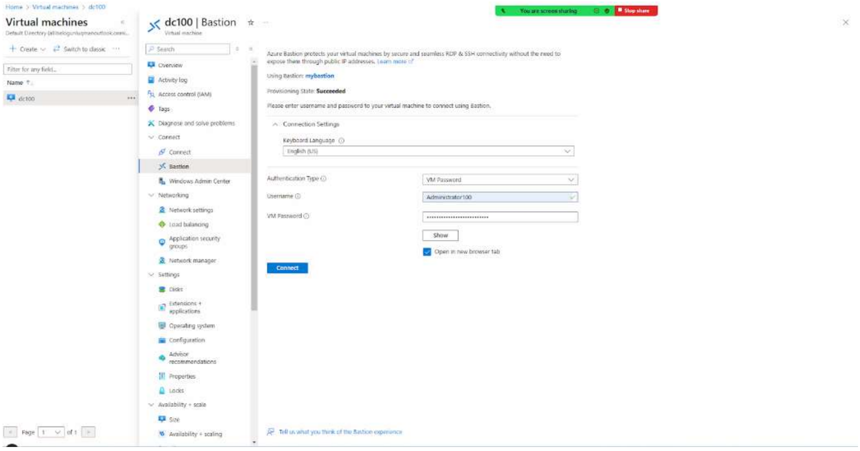
Azure disk encryption : Not enabled

Figure 9: Virtual Machine After Deployment

2.1 Establishing RDP Connection

Using Azure Bastion, users could securely establish a Remote Desktop Protocol (RDP) connection to the virtual machine directly from the Azure portal. Unlike traditional RDP methods that require exposing the VM to the internet, Azure Bastion eliminates the need for a public IP address, reducing security risks while enabling seamless remote access.

This approach ensures a more secure and efficient remote management process by allowing users to interact with the virtual machine without relying on external RDP clients. Figures 2.4 to 2.5 illustrate the steps involved in establishing the Bastion-powered RDP connection.



Azure Bastion protects your virtual machines by secure and seamless RDP & SSH connectivity without the need to expose them through public IP addresses. Learn more

Using Bastion: **mybastion**

Provisioning State: **Succeeded**

Please enter username and password to your virtual machine to connect using Bastion.

Connection Settings

Keyboard Language: English (US)

Authentication Type: VM Password

Username: Administrator100

VM Password: ••••••••••••••••••••••••••

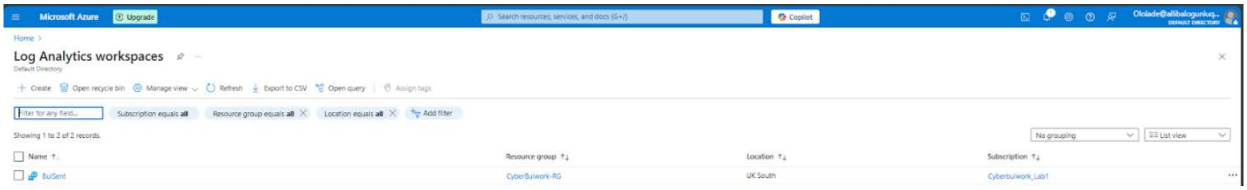
☑ Open in new browser tab

Figure 10: RDP connection using Azure Bastion

Figure 11: Image of the VM via Bastion

2.2 Connecting the Virtual Machine to Log Analytics

Azure Log Analytics provides a centralized platform for collecting, analyzing, and visualizing log and telemetry data from various sources. This enables better insights into the performance, security, and compliance of the deployed cloud environment. By connecting the VM to Log Analytics, we established real-time monitoring and analysis of system logs, ensuring proactive issue detection and resolution while improving security monitoring and operational efficiency in the cloud environment.

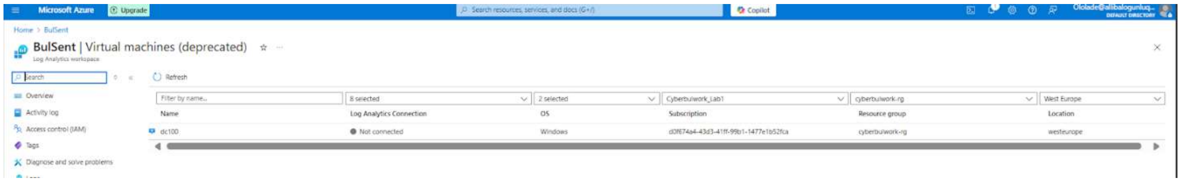


Subscription equals **all** | Resource group equals **all** | Location equals **all**

Showing 1 to 2 of 2 records.

Name	Resource group	Location	Subscription
BulSent	CyberBulwork-RG	UK South	Cyberbulwork_Lab1

Figure 12: Selecting the VM in the Log Analytics Workspace

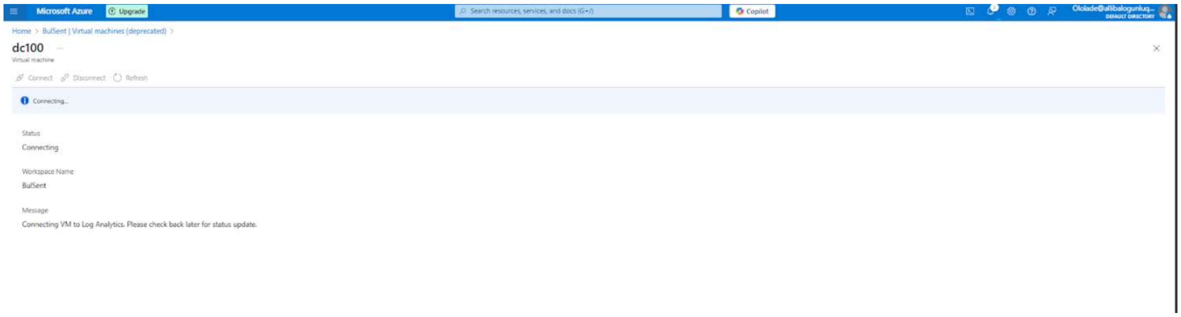


BulSent | Virtual machines (deprecated)

Log Analytics workspace

Name	Log Analytics Connection	OS	Subscription	Resource group	Location
dc100	● Not connected	Windows	d0f674a4-43d3-41ff-99b1-1477e1b52fca	cyberbulwork-rg	westeurope

Figure 13: Display of the VM in a disconnected state


Microsoft Azure
Upgrade
Search resources, services, and docs (G+/)
Copilot
Ololade@allibalogunluq...
DEFAULT DIRECTORY
Home > BulSent | Virtual machines (deprecated) >
Connect
Disconnect
Refresh

dc100

Virtual machine

Connecting...

Status

Connecting

Workspace Name

BulSent

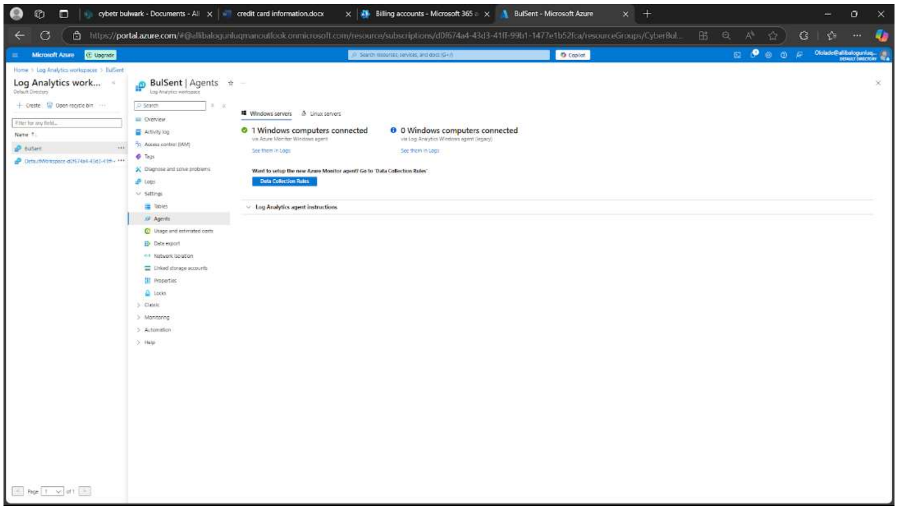
Message

Connecting VM to Log Analytics. Please check back later for status update.

Figure 14: Connecting the VM to Microsoft Sentinel

2.3 Connecting the VM to Agent Management

Azure agents facilitate communication between resources and Azure services for monitoring and control. Establishing this connection allows the virtual machine to transmit logs to Microsoft Sentinel for continuous monitoring and security analysis. The setup process ensures real-time visibility into system activities, enabling proactive threat detection and incident response. The connection is shown in the figures below.



BulSent | Agents

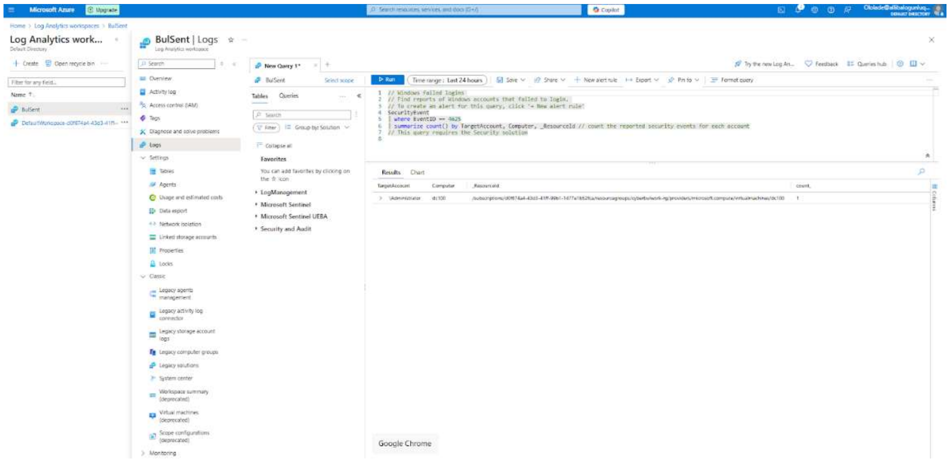
Windows servers Linux servers

1 Windows computers connected
via Azure Monitor Windows agent
See them in Logs

0 Windows computers connected
via Log Analytics Windows agent (legacy)
See them in Logs

Want to setup the new Azure Monitor agent? Go to 'Data Collection Rules'

Figure 15: Display of the VM Connected to Agent Management



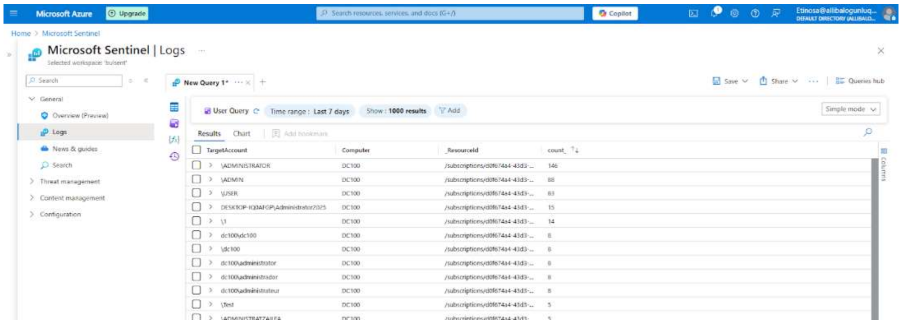
BulSent | Logs

Time range : Last 24 hours

```
// Windows failed logins
// Find reports of Windows accounts that failed to login.
// To create an alert for this query, click '+ New alert rule'
SecurityEvent
| where EventID == 4625
| summarize count() by TargetAccount, Computer, _ResourceId // count the reported security events for each account
// This query requires the Security solution
```

TargetAccount	Computer	_ResourceId	count_
\Administrator	dc100	/subscriptions/d0f674a4-43d3-41ff-99b1-1477e1b52fca/resourcegroups/cyberbulwark-rg/providers/microsoft.compute/virtualmachines/dc100	1

Figure 16: The log management showing captured logs



Microsoft Sentinel | Logs

User Query Time range : Last 7 days Show : 1000 results

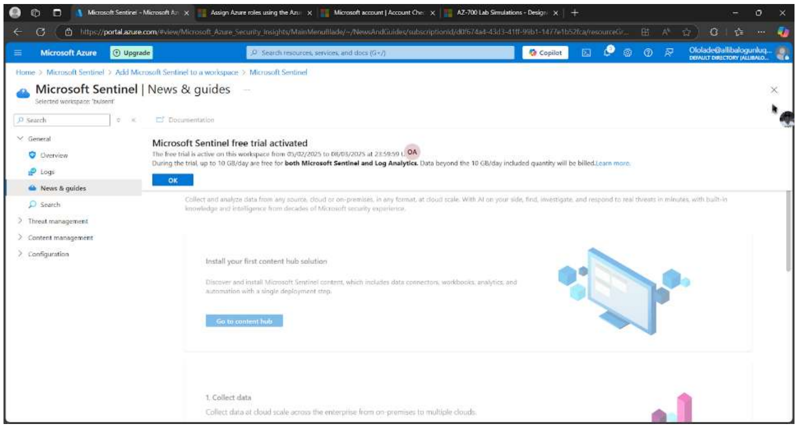
TargetAccount	Computer	_ResourceId	count_
\ADMINISTRATOR	DC100	/subscriptions/d0f674a4-43d3-...	146
\ADMIN	DC100	/subscriptions/d0f674a4-43d3-...	88
\USER	DC100	/subscriptions/d0f674a4-43d3-...	63
DESKTOP-IQ0AFGP\Administrator2025	DC100	/subscriptions/d0f674a4-43d3-...	15
\1	DC100	/subscriptions/d0f674a4-43d3-...	14
dc100\dc100	DC100	/subscriptions/d0f674a4-43d3-...	8
\dc100	DC100	/subscriptions/d0f674a4-43d3-...	8
dc100\administrator	DC100	/subscriptions/d0f674a4-43d3-...	8
dc100\administrador	DC100	/subscriptions/d0f674a4-43d3-...	8
dc100\administrateur	DC100	/subscriptions/d0f674a4-43d3-...	8
\Test	DC100	/subscriptions/d0f674a4-43d3-...	5
\ADMINISTRATZAILEA	DC100	/subscriptions/d0f674a4-43d3-...	5

Figure 17: DDOS attack on the VM logs

2.4 Connecting the Virtual Machine to Microsoft Sentinel

Microsoft Sentinel is a cloud-native Security Information and Event Management (SIEM) solution designed to aggregate and analyze data from multiple sources, enabling proactive threat detection, incident investigation, and enhanced security management.

By leveraging Microsoft Sentinel's data connectors, organizations can seamlessly integrate various data sources, ensuring comprehensive monitoring and analysis across their entire infrastructure. This integration strengthens security posture by providing real-time insights, automated threat detection, and streamlined incident response mechanisms.



Microsoft Sentinel | News & guides

Selected workspace: 'bulsent'

Microsoft Sentinel free trial activated

The free trial is active on this workspace from 05/02/2025 to 08/03/2025 at 23:59:59 U

During the trial, up to 10 GB/day are free for **both Microsoft Sentinel and Log Analytics.** Data beyond the 10 GB/day included quantity will be billed.Learn more.

Collect and analyze data from any source, cloud or on-premises, in any format, at cloud scale. With AI on your side, find, investigate, and respond to real threats in minutes, with built-in knowledge and intelligence from decades of Microsoft security experience.

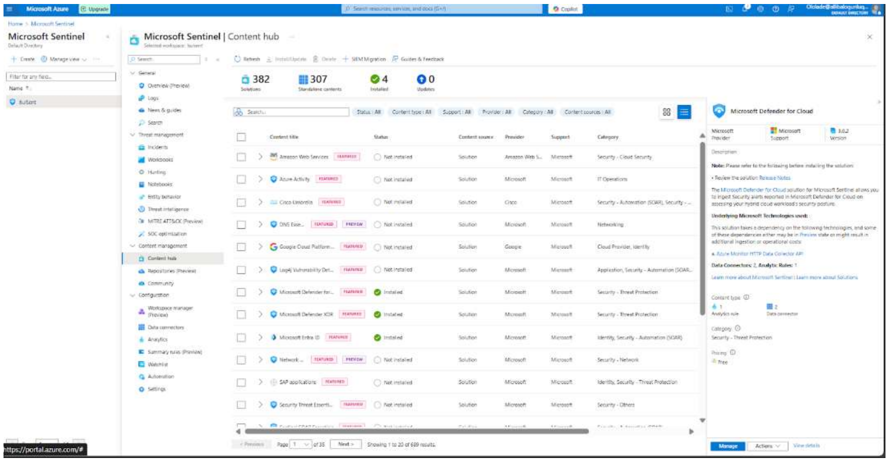
Install your first content hub solution

Discover and install Microsoft Sentinel content, which includes data connectors, workbooks, analytics, and automation with a single deployment step.

1. Collect data

Collect data at cloud scale across the enterprise from on-premises to multiple clouds.

Figure 18: Microsoft Sentinel is accessed to enhance security event management.



Microsoft Sentinel | Content hub

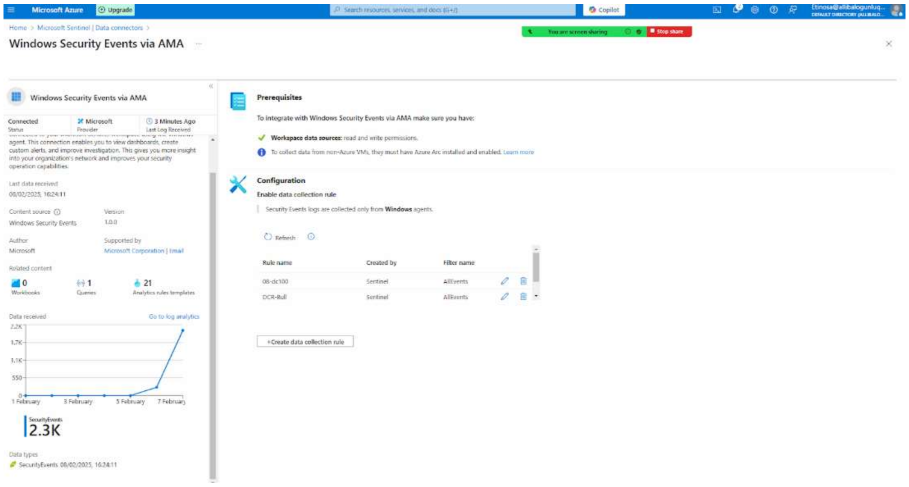
382 Solutions | 307 Standalone contents | 4 Installed | 0 Updates

Content title	Status	Content source	Provider	Support	Category
Amazon Web Services FEATURED	Not installed	Solution	Amazon Web S...	Microsoft	Security - Cloud Security
Azure Activity FEATURED	Not installed	Solution	Microsoft	Microsoft	IT Operations
Cisco Umbrella FEATURED	Not installed	Solution	Cisco	Microsoft	Security - Automation (SOAR), Security - ...
DNS Esse... FEATURED PREVIEW	Not installed	Solution	Microsoft	Microsoft	Networking
Google Cloud Platform... FEATURED	Not installed	Solution	Google	Microsoft	Cloud Provider, Identity
Log4j Vulnerability Det... FEATURED	Not installed	Solution	Microsoft	Microsoft	Application, Security - Automation (SOAR...
Microsoft Defender for... FEATURED	Installed	Solution	Microsoft	Microsoft	Security - Threat Protection
Microsoft Defender XDR FEATURED	Installed	Solution	Microsoft	Microsoft	Security - Threat Protection
Microsoft Entra ID FEATURED	Installed	Solution	Microsoft	Microsoft	Identity, Security - Automation (SOAR)
Network ... FEATURED PREVIEW	Not installed	Solution	Microsoft	Microsoft	Security - Network
SAP applications FEATURED	Not installed	Solution	Microsoft	Microsoft	Identity, Security - Threat Protection
Security Threat Essenti... FEATURED	Not installed	Solution	Microsoft	Microsoft	Security - Others

Page 1 of 35 Showing 1 to 20 of 689 results.

Microsoft Defender for Cloud

Figure 19: Sentinel Installed Solutions



Microsoft Azure
Upgrade
Search resources, services, and docs (G+/)
Copilot
Etinosa@alibaloguniuq...
DEFAULT DIRECTORY (ALLIBALO...
You are screen sharing
Stop share
Home > Microsoft Sentinel | Data connectors >

Windows Security Events via AMA

Windows Security Events via AMA

Connected
Status

Microsoft
Provider

3 Minutes Ago
Last Log Received

agent. This connection enables you to view dashboards, create custom alerts, and improve investigation. This gives you more insight into your organization's network and improves your security operation capabilities.

Last data received
08/02/2025, 16:24:11

Content source: Windows Security Events

Version: 1.0.0

Author: Microsoft

Supported by: Microsoft Corporation | Email

Related content

0 Workbooks

1 Queries

21 Analytics rules templates

Data types
SecurityEvents 08/02/2025, 16:24:11

Prerequisites

To integrate with Windows Security Events via AMA make sure you have:

✓ **Workspace data sources:** read and write permissions.

To collect data from non-Azure VMs, they must have Azure Arc installed and enabled. Learn more

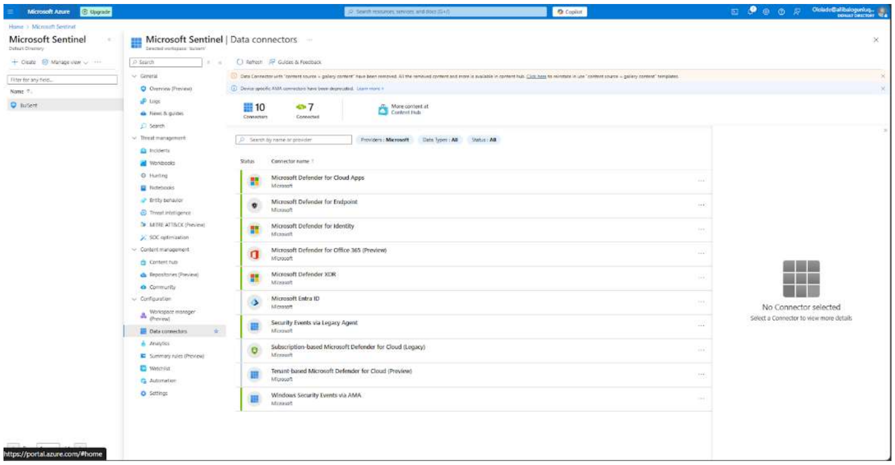
Configuration

Enable data collection rule

Security Events logs are collected only from **Windows** agents.

Rule name	Created by	Filter name
08-dc100	Sentinel	AllEvents
DCR-Bull	Sentinel	AllEvents

Figure 20: Microsoft AMA Onboarding



Data Connector with "content source = gallery content" have been removed. All the removed content and more is available in content hub. Click here to reinstate in use "content source = gallery content" templates.

Device specific AMA connectors have been deprecated. Learn more >

10 Connectors

7 Connected

More content at Content Hub

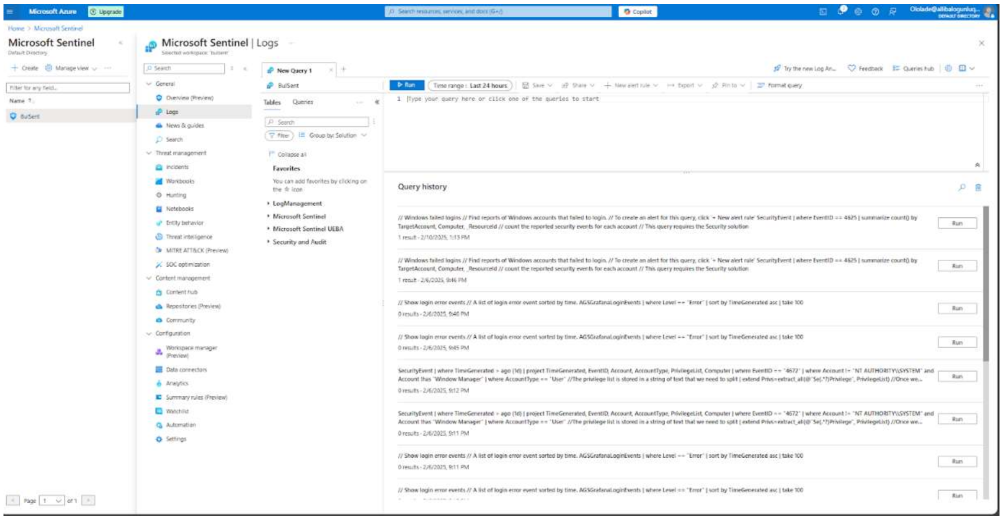
Providers : **Microsoft** Data Types : **All** Status : **All**

Status	Connector name
	Microsoft Defender for Cloud Apps Microsoft
	Microsoft Defender for Endpoint Microsoft
	Microsoft Defender for Identity Microsoft
	Microsoft Defender for Office 365 (Preview) Microsoft
	Microsoft Defender XDR Microsoft
	Microsoft Entra ID Microsoft
	Security Events via Legacy Agent Microsoft
	Subscription-based Microsoft Defender for Cloud (Legacy) Microsoft
	Tenant-based Microsoft Defender for Cloud (Preview) Microsoft
	Windows Security Events via AMA Microsoft

No Connector selected

Select a Connector to view more details

Figure 21: Windows Security Events Data Connectors Installed on Microsoft Sentinel.



Query history

```
// Windows failed logins // Find reports of Windows accounts that failed to login. // To create an alert for this query, click '+ New alert rule' SecurityEvent | where EventID == 4625 | summarize count() by TargetAccount, Computer, _ResourceId // count the reported security events for each account // This query requires the Security solution
1 result - 2/10/2025, 1:13 PM

// Windows failed logins // Find reports of Windows accounts that failed to login. // To create an alert for this query, click '+ New alert rule' SecurityEvent | where EventID == 4625 | summarize count() by TargetAccount, Computer, _ResourceId // count the reported security events for each account // This query requires the Security solution
1 result - 2/6/2025, 9:46 PM

// Show login error events // A list of login error event sorted by time. AGSGrafanaLoginEvents | where Level == "Error" | sort by TimeGenerated asc | take 100
0 results - 2/6/2025, 9:46 PM

// Show login error events // A list of login error event sorted by time. AGSGrafanaLoginEvents | where Level == "Error" | sort by TimeGenerated asc | take 100
0 results - 2/6/2025, 9:45 PM

SecurityEvent | where TimeGenerated > ago (1d) | project TimeGenerated, EventID, Account, AccountType, PrivilegeList, Computer | where EventID == "4672" | where Account != "NT AUTHORITY\\SYSTEM" and Account !has "Window Manager" | where AccountType == "User" //The privilege list is stored in a string of text that we need to split | extend Privs=extract_all(@"Se(.*?)Privilege", PrivilegeList) //Once we...
0 results - 2/6/2025, 9:12 PM

SecurityEvent | where TimeGenerated > ago (1d) | project TimeGenerated, EventID, Account, AccountType, PrivilegeList, Computer | where EventID == "4672" | where Account != "NT AUTHORITY\\SYSTEM" and Account !has "Window Manager" | where AccountType == "User" //The privilege list is stored in a string of text that we need to split | extend Privs=extract_all(@"Se(.*?)Privilege", PrivilegeList) //Once we...
0 results - 2/6/2025, 9:11 PM

// Show login error events // A list of login error event sorted by time. AGSGrafanaLoginEvents | where Level == "Error" | sort by TimeGenerated asc | take 100
0 results - 2/6/2025, 9:11 PM

// Show login error events // A list of login error event sorted by time. AGSGrafanaLoginEvents | where Level == "Error" | sort by TimeGenerated asc | take 100
```

Figure 22: Details of log activity captures.

2.5 Challenges Encountered

During the implementation of Microsoft Sentinel for security monitoring and log analysis, the team faced several challenges that required strategic solutions. These challenges primarily revolved around optimizing threat detection accuracy and managing log retention effectively.

- **Fine-Tuning Sentinel to Reduce False Positives:** Configuring Microsoft Sentinel to minimize false positives proved challenging, requiring continuous adjustments to alert rules and policies to ensure accurate threat detection without unnecessary noise.
- **Managing Log Storage and Retention Policies:** Balancing storage costs with the need for comprehensive log retention was another challenge, necessitating strategic planning to optimize storage usage while maintaining compliance and security standards.

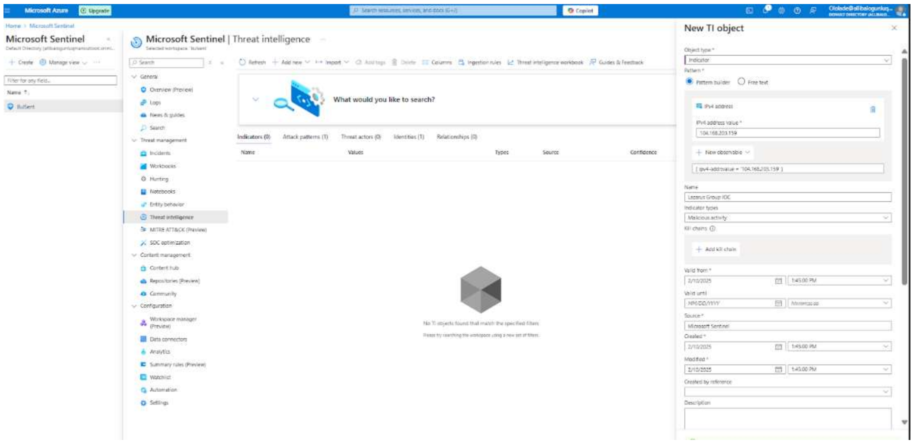
Results and Findings

Despite these challenges, the implementation of Microsoft Sentinel yielded significant improvements in security monitoring:

- **Improved Visibility:** Microsoft Sentinel provided enhanced insight into user activities and cloud resource interactions, allowing for better monitoring and security enforcement.
- **Threat Detection and Analysis:** Through log analysis, key patterns and potential security threats were identified, enabling proactive incident response and strengthening overall security posture.

Security Incident and Event Management (SIEM)

Microsoft Sentinel is a cloud-native Security Information and Event Management (SIEM) tool available on Azure Cloud Services, designed to enable seamless ingestion of logs from both on-premise and cloud infrastructures. It provides real-time threat detection, intelligent security analytics, and automated response capabilities, helping organizations enhance their security posture by identifying and mitigating potential risks efficiently.



Object type *: Indicator

Pattern *: ● Pattern builder ○ Free text

IPv4 address

IPv4 address value *: 104.168.203.159

[ipv4-addr:value = '104.168.203.159']

Name: Lazarus Group IOC

Indicator types: Malicious activity

Valid from *: 2/10/2025 1:45:00 PM

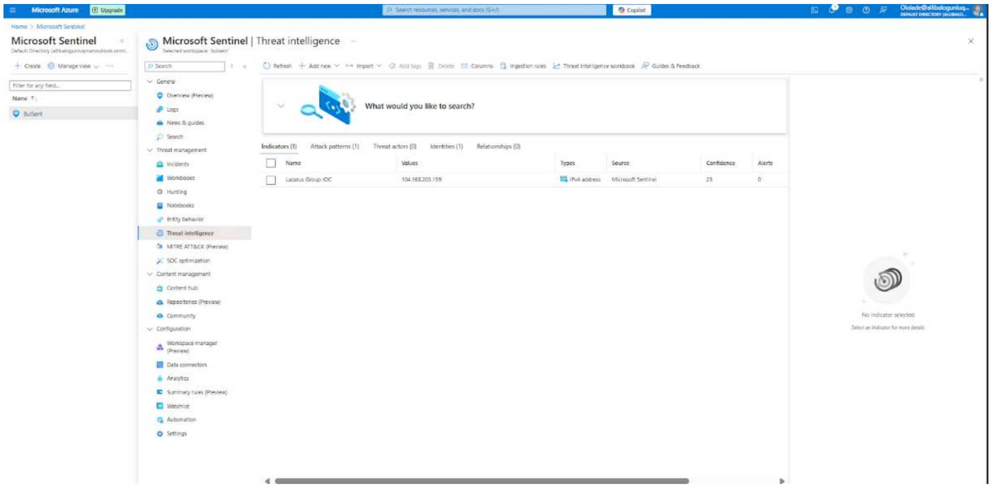
Valid until: MM/DD/YYYY hh:mm:ss aa

Source *: Microsoft Sentinel

Created *: 2/10/2025 1:45:00 PM

Modified *: 2/10/2025 1:45:00 PM

Figure 23: Adding a threat Indicator



Name	Values	Types	Source	Confidence	Alerts
Lazarus Group IOC	104.168.203.159	IPv4 address	Microsoft Sentinel	25	0

Figure 24: Indicators, Attack patterns and Identities Added

3.1 Benefits of Tagging Threat Indicators

Tagging threat indicators in Microsoft Sentinel offers several advantages that enhance threat detection, incident response, and overall security management:

1. **Efficient Threat Prioritization**
    - Categorizes threats based on factors like severity, type, location, and affected assets.
    - Enables security teams to prioritize threats quickly by tagging specific sources for easy identification.
2. **Automated Anomaly Detection & Faster Response**
    - Security tools leveraging tagged indicators can automatically detect anomalies linked to known threats.
    - Reduces incident response time and minimizes the risk of potential breaches.
3. **Improved Search, Analysis, and Threat Hunting**
    - Helps security teams quickly search, retrieve, and analyze relevant threat data.
    - Supports proactive threat hunting and enhances decision-making.
4. **Standardized Labeling & Categorization**
    - Ensures consistent threat intelligence data handling across all Azure environments.
    - Facilitates better collaboration between teams managing cybersecurity.
5. **Regulatory Compliance & Reporting**
    - Helps organizations demonstrate compliance with industry regulations and internal policies.
    - Aids in generating detailed reports on threat detection and response efforts.

By implementing threat tagging, organizations can enhance security visibility, improve response efficiency, and strengthen their cybersecurity posture within Microsoft Sentinel.

Data Loss Prevention Policy

The rapid shift to cloud-based operations has transformed how organizations store, manage, and share data. However, this digital evolution introduces a critical challenge: protecting sensitive information from unauthorized access, accidental leaks, and data breaches. The consequences of data loss can be severe, leading to regulatory penalties, reputational damage, and financial setbacks.

To combat these risks, Microsoft Data Loss Prevention (DLP) provides a comprehensive security framework on the Azure platform, ensuring that organizations can identify, monitor, and safeguard sensitive data across diverse environments. With automated policies, real-time alerts, and proactive enforcement mechanisms, Microsoft DLP enhances data security, strengthens compliance, and minimizes the risk of exposure. By integrating DLP into their cloud infrastructure, businesses can proactively mitigate threats, maintain regulatory compliance, and ensure data integrity in an increasingly complex digital landscape.

4.1 Key Benefits of Microsoft Purview Data Loss Prevention (DLP)

Microsoft Purview DLP is a powerful solution designed to protect sensitive data across various platforms, ensuring compliance and security. Here are its key benefits:

1. Comprehensive Data Protection

- Prevents unauthorized sharing or transfer of sensitive information across cloud services, endpoints, and emails.
- Enforces real-time policy controls to restrict data leaks in Microsoft 365, Teams, SharePoint, and OneDrive.

2. Advanced Data Classification & Sensitivity Labels

- Uses machine learning and AI-driven classification to detect and protect confidential information (e.g., PII, financial data, intellectual property).
- Supports custom sensitivity labels to apply appropriate security measures based on data classification.

3. Unified Policy Enforcement Across Platforms

- Ensures consistent data protection across Microsoft services, including Azure, Exchange, Teams, and non-Microsoft environments through built-in integrations.
- Provides a single-pane-of-glass management interface for streamlined policy creation and enforcement.

4. Regulatory Compliance & Risk Mitigation

- Helps organizations comply with GDPR, HIPAA, ISO 27001, CCPA, and other regulatory requirements by preventing data exposure.
- Offers audit logs and incident reports to track compliance and potential violations.

5. Intelligent Alerts & Automated Remediation

- Detects and flags suspicious data activity in real time, reducing the risk of insider threats and accidental leaks.
- Provides automated remediation actions, such as blocking unauthorized sharing, encrypting sensitive files, or notifying security teams.

6. Endpoint Data Protection

- Extends DLP policies to Windows, macOS, and mobile devices to prevent copy-pasting, printing, or transferring sensitive files via USB drives or cloud storage.
- Ensures data security even when users are offline or outside the corporate network.

7. Seamless Integration with Microsoft Defender & Sentinel

- Works with Microsoft Defender for Cloud Apps to enhance data visibility and threat detection.
- Integrates with Microsoft Sentinel for security monitoring and analytics, strengthening an organization's security posture.

8. User Education & Adaptive Controls

- Provides user-friendly prompts and justifications, helping employees make informed decisions while handling sensitive data.
- Encourages secure collaboration without disrupting productivity.

By implementing Microsoft Purview DLP, organizations can enhance their data security, regulatory compliance, and risk management strategies, ensuring that sensitive information remains protected across cloud, email, and endpoint environments.

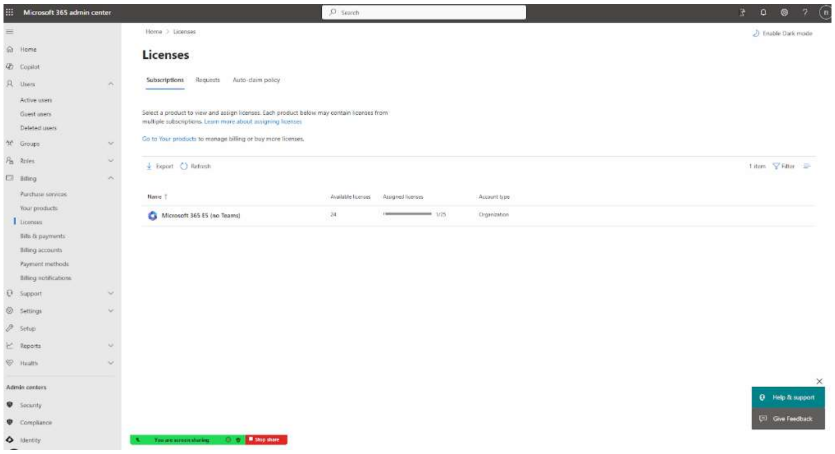
4.2 Configuring and Creating DLP Policy

As part of its cloud migration strategy, CyberBulwork has prioritized the protection of sensitive data by implementing a Data Loss Prevention (DLP) policy. This policy is designed to detect, warn, and block the transmission of emails containing confidential company information, employee details, or executable files, preventing potential data breaches.

To enable DLP enforcement, a Microsoft Purview account was created using the Owner's account, ensuring seamless integration of all Azure users into the Purview portal. Additionally, a Microsoft 365 Business Premium subscription was activated, unlocking DLP capabilities within the Purview Compliance portal.

Following the setup, role-based access was assigned to the Compliance Manager and Cybersecurity Manager, granting them the authority to configure and manage DLP policies. These policies establish security controls that monitor, restrict, and protect sensitive data across CyberBulwork's cloud environment.

The full configuration process is illustrated in **Figures 25 to 30** below.



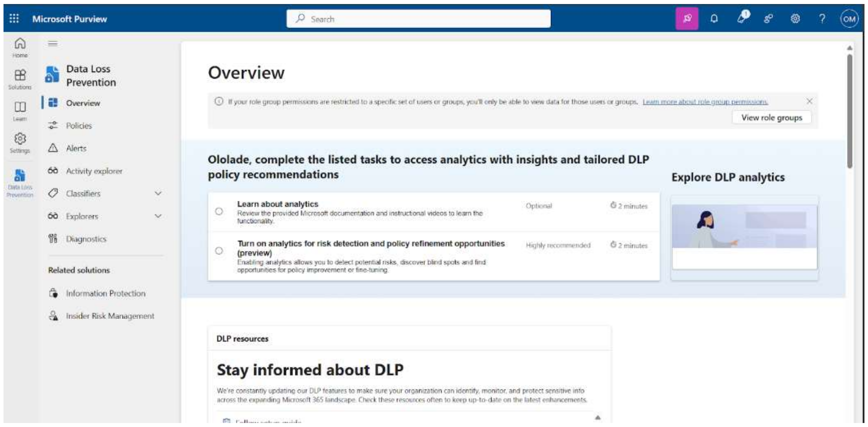
Licenses

Select a product to view and assign licenses. Each product below may contain licenses from multiple subscriptions. Learn more about assigning licenses

Go to Your products to manage billing or buy more licenses.

Name	Available licenses	Assigned licenses	Account type
Microsoft 365 E5 (no Teams)	24	1/25	Organization

Figure 25: Microsoft E5 license purchase



Overview

If your role group permissions are restricted to a specific set of users or groups, you'll only be able to view data for those users or groups. Learn more about role group permissions.

Ololade, complete the listed tasks to access analytics with insights and tailored DLP policy recommendations

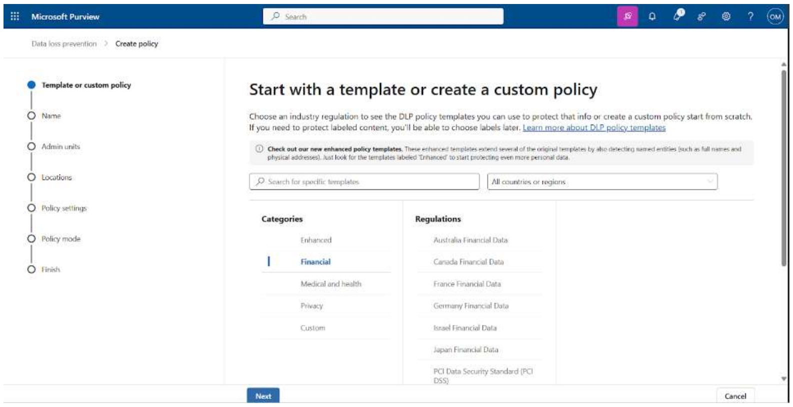
○ **Learn about analytics** — Optional — 2 minutes
Review the provided Microsoft documentation and instructional videos to learn the functionality.

○ **Turn on analytics for risk detection and policy refinement opportunities (preview)** — Highly recommended — 2 minutes
Enabling analytics allows you to detect potential risks, discover blind spots and find opportunities for policy improvement or fine-tuning.

Stay informed about DLP

We're constantly updating our DLP features to make sure your organization can identify, monitor, and protect sensitive info across the expanding Microsoft 365 landscape. Check these resources often to keep up-to-date on the latest enhancements.

Figure 26: Microsoft Purview Overview



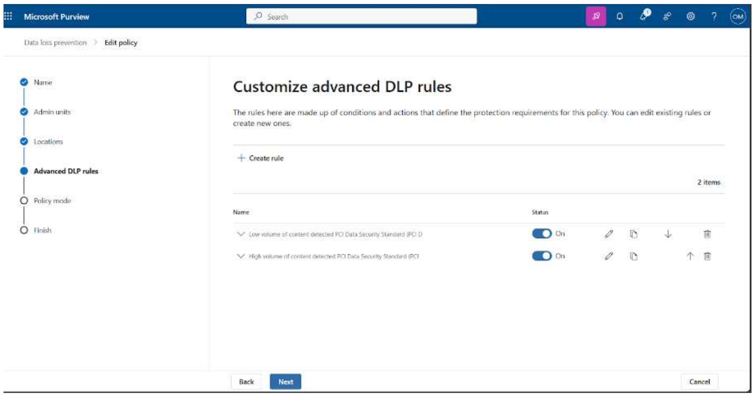
Start with a template or create a custom policy

Choose an industry regulation to see the DLP policy templates you can use to protect that info or create a custom policy start from scratch. If you need to protect labeled content, you'll be able to choose labels later. Learn more about DLP policy templates

Check out our new enhanced policy templates. These enhanced templates extend several of the original templates by also detecting named entities (such as full names and physical addresses). Just look for the templates labeled 'Enhanced' to start protecting even more personal data.

Categories	Regulations
Enhanced	Australia Financial Data
Financial	Canada Financial Data
Medical and health	France Financial Data
Privacy	Germany Financial Data
Custom	Israel Financial Data
	Japan Financial Data
	PCI Data Security Standard (PCI DSS)

Figure 27: Creating the DLP Policy



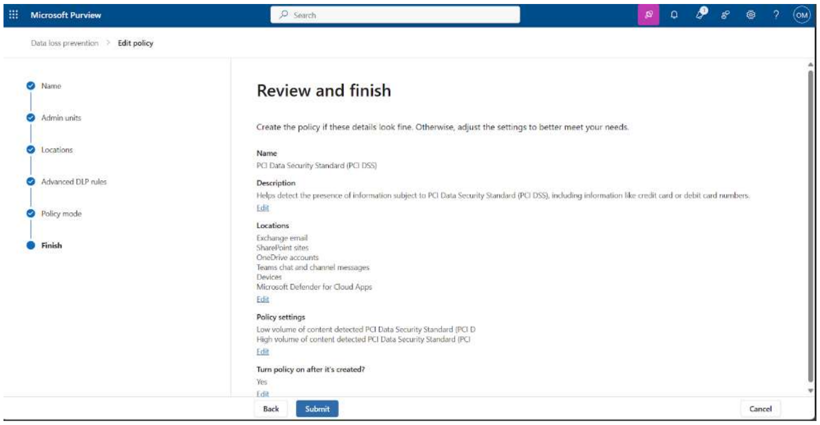
Customize advanced DLP rules

The rules here are made up of conditions and actions that define the protection requirements for this policy. You can edit existing rules or create new ones.

2 items

Name	Status
Low volume of content detected PCI Data Security Standard (PCI D	On
High volume of content detected PCI Data Security Standard (PCI	On

Figure 28: Configuring Advanced Rules for the DLP Policy



Review and finish

Create the policy if these details look fine. Otherwise, adjust the settings to better meet your needs.

Name
PCI Data Security Standard (PCI DSS)

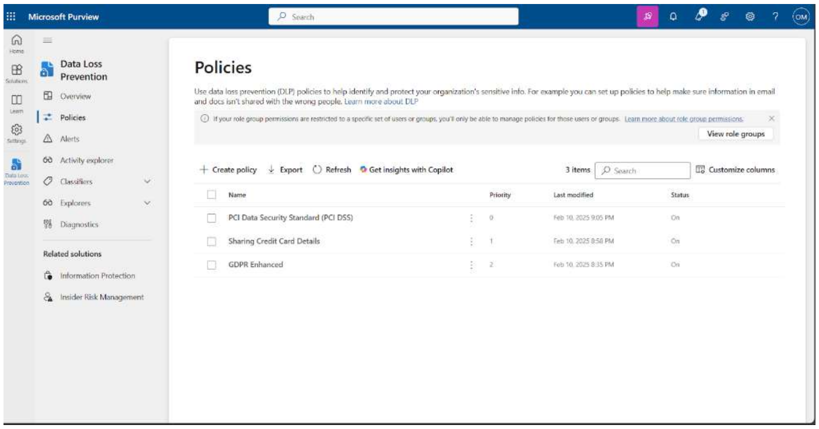
Description
Helps detect the presence of information subject to PCI Data Security Standard (PCI DSS), including information like credit card or debit card numbers.
Edit

Locations
Exchange email
SharePoint sites
OneDrive accounts
Teams chat and channel messages
Devices
Microsoft Defender for Cloud Apps
Edit

Policy settings
Low volume of content detected PCI Data Security Standard (PCI D
High volume of content detected PCI Data Security Standard (PCI
Edit

Turn policy on after it's created?
Yes
Edit

Figure 29: Review and finish the DPL policy



Policies

Use data loss prevention (DLP) policies to help identify and protect your organization's sensitive info. For example you can set up policies to help make sure information in email and docs isn't shared with the wrong people. Learn more about DLP

If your role group permissions are restricted to a specific set of users or groups, you'll only be able to manage policies for those users or groups. Learn more about role group permissions.

3 items

Name	Priority	Last modified	Status
PCI Data Security Standard (PCI DSS)	0	Feb 10, 2025 9:05 PM	On
Sharing Credit Card Details	1	Feb 10, 2025 8:58 PM	On
GDPR Enhanced	2	Feb 10, 2025 8:35 PM	On

Figure 30: Some of the DLP Policies Created on Microsoft Purview

4.3 How Microsoft Purview DLP Detects Sensitive Information in an Organization

In an organization, data security and compliance are critical to safeguarding sensitive information from unauthorized access, accidental leaks, and cyber threats. Microsoft Purview Data Loss Prevention (DLP) plays a key role in detecting and protecting sensitive data across an organization's cloud environment, endpoints, and communication channels.

1. Identifying Sensitive Data

Purview DLP detects:

- Financial Data: Credit card details, bank accounts.
- PII: Employee/customer records, national IDs.

- Health Information: Medical and insurance data.
- Confidential Business Documents: Contracts, trade secrets.

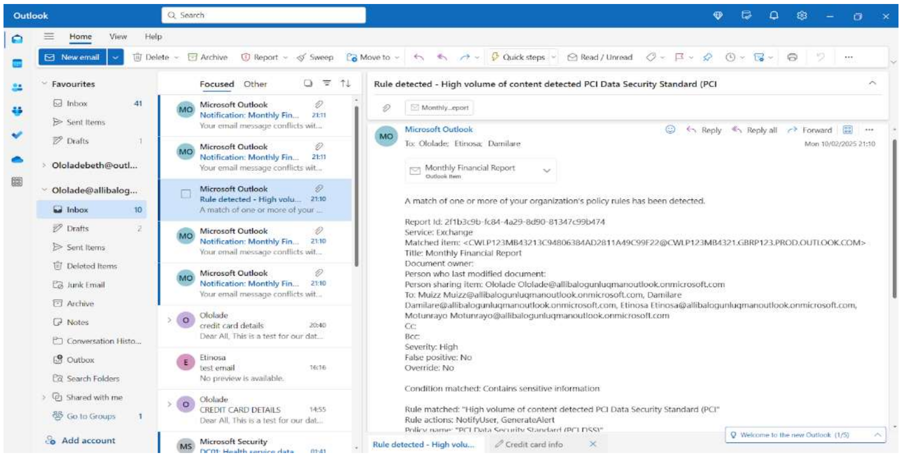
2. Monitoring and Enforcement

Purview DLP prevents data leaks by scanning:

- Emails & Messaging (Exchange, Teams) – Blocks unauthorized sharing.
- Cloud Storage (OneDrive, SharePoint) – Restricts access to sensitive files.
- Endpoints (Laptops, Devices) – Monitors file transfers and printing.

3. Advanced Detection & Compliance

- Pattern Matching & Content Inspection – Identifies structured and unstructured sensitive data.
- Automated Policy Enforcement – Blocks risky actions, notifies users, and encrypts sensitive files.
- Integration with Security Tools – Works with Defender for Cloud Apps and Azure Information Protection for enhanced security.



Microsoft Outlook
Notification: Monthly Fin... 21:11
Your email message conflicts wit...

Microsoft Outlook
Notification: Monthly Fin... 21:11
Your email message conflicts wit...

Microsoft Outlook
Rule detected - High volu... 21:10
A match of one or more of your ...

Microsoft Outlook
Notification: Monthly Fin... 21:10
Your email message conflicts wit...

Microsoft Outlook
Notification: Monthly Fin... 21:10
Your email message conflicts wit...

Ololade
credit card details 20:40
Dear All, This is a test for our dat...

Etinosa
test email 16:16
No preview is available.

Ololade
CREDIT CARD DETAILS 14:55
Dear All, This is a test for our dat...

Microsoft Security
DC01: Health service data 01:41

Rule detected - High volume of content detected PCI Data Security Standard (PCI

Monthly...eport

Microsoft Outlook
To: Ololade; Etinosa; Damilare
Mon 10/02/2025 21:10

Monthly Financial Report
Outlook item

A match of one or more of your organization's policy rules has been detected.

Report Id: 2f1b3c9b-fc84-4a29-8d90-81347c99b474
Service: Exchange
Matched item: <CWLP123MB43213C94806384AD2811A49C99F22@CWLP123MB4321.GBRP123.PROD.OUTLOOK.COM>
Title: Monthly Financial Report
Document owner:
Person who last modified document:
Person sharing item: Ololade Ololade@allibalogunluqmanoutlook.onmicrosoft.com
To: Muizz Muizz@allibalogunluqmanoutlook.onmicrosoft.com, Damilare Damilare@allibalogunluqmanoutlook.onmicrosoft.com, Etinosa Etinosa@allibalogunluqmanoutlook.onmicrosoft.com, Motunrayo Motunrayo@allibalogunluqmanoutlook.onmicrosoft.com
Cc:
Bcc:
Severity: High
False positive: No
Override: No

Condition matched: Contains sensitive information

Rule matched: "High volume of content detected PCI Data Security Standard (PCI"
Rule actions: NotifyUser, GenerateAlert
Policy name: "PCI Data Security Standard (PCI DSS)"

Rule detected - High volu...
Credit card info

Figure 31: Notification sent showcasing that the policy has been breached

4.4 Challenges Encountered During DLP Policy Configuration

1. **DLP Tab Not Visible on the Compliance Page:** After setting up the Purview account, the DLP tab was missing from the Compliance page, with no clear guidance on how to enable it. This delayed the configuration process.

2. **Role Assignment Issues:** Despite configuring Microsoft 365, key compliance features remained inaccessible. It was later discovered that DLP role assignments had to be manually configured in the **Purview Admin Manager**, a step not initially documented.
3. **DLP Policy Implementation Challenges:** Policies created using built-in templates did not trigger expected alerts or actions during testing. Troubleshooting revealed gaps in policy configuration that required additional fine-tuning.
4. **Email Format Compatibility Issues:** The DLP policies failed to detect sensitive information in emails. After extensive troubleshooting, it was discovered that the issue stemmed from an incorrect email format, requiring adjustments for proper detection.

Addressing the Challenges

1. **Enabling the DLP Tab on the Compliance Page:** To resolve the missing DLP tab issue, we ensured that the correct Microsoft 365 Business Premium subscription was active. We also verified that Purview compliance features were correctly provisioned, which enabled the tab to appear.
2. **Configuring Role Assignments:** We navigated to the Purview Admin Center and manually assigned the required DLP role permissions to the Compliance Manager and Cybersecurity Manager. This granted the necessary access to configure and manage DLP policies.
3. **Troubleshooting DLP Policy Actions:** To ensure policies triggered the intended alerts and actions, we reviewed the policy conditions, rules, and enforcement settings. We also conducted multiple test scenarios and fine-tuned the configurations to align with organizational data security requirements.
4. **Fixing Email Format Detection Issues:** After extensive troubleshooting, we discovered that the email format did not align with the DLP policy detection criteria. We adjusted the formatting, ensuring that policies correctly identified and flagged sensitive information in outgoing emails.

4.5 Implementation of Azure AD DS

Migrating on-premises users to Azure Active Directory (Azure AD) ensures centralized identity management and seamless authentication across cloud and on-prem environments. By leveraging Microsoft Entra Connect, we synchronized our existing directory while maintaining security and compliance.

Deployment Process

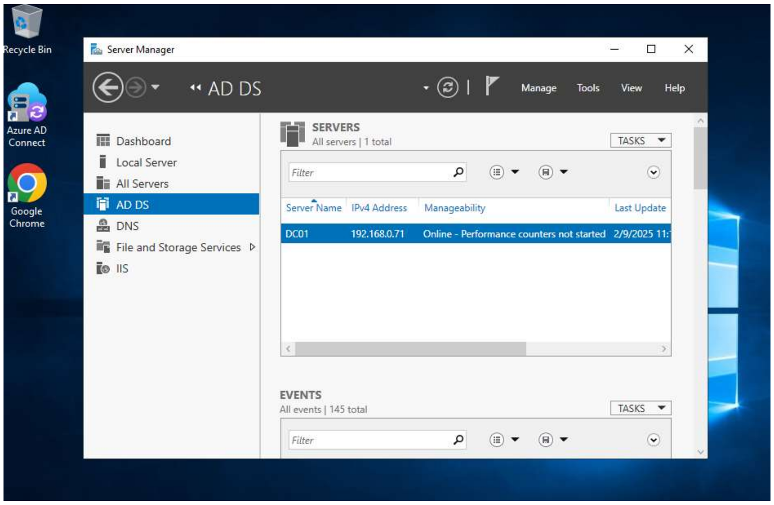
To prepare for migration, we configured Windows Server 2019 Datacenter, enabled Active Directory Domain Services (AD DS), and installed Microsoft IdFix to resolve directory inconsistencies.

We ensured global admin privileges were assigned in both Azure Entra and on-prem AD, along with a stable internet connection for synchronization.

We then downloaded and installed Microsoft Entra Connect, selecting Custom Settings for advanced configurations. Authentication was established using Azure AD Global Admin and on-prem AD credentials, and Password Hash Sync was enabled to allow seamless login experiences.

During configuration, we filtered specific users, groups, and Organizational Units (OUs) to synchronize. Once installation was completed, Microsoft Entra Connect initiated the first synchronization, ensuring a smooth transition. To validate the migration, we monitored sync status using the Microsoft Entra Connect Synchronization Service and verified user entries in Azure AD via the Azure Portal.

This approach streamlined the migration, enabling secure and efficient identity synchronization between on-premises and cloud environments. The full configuration process is illustrated in **Figures 32 to 42** below.

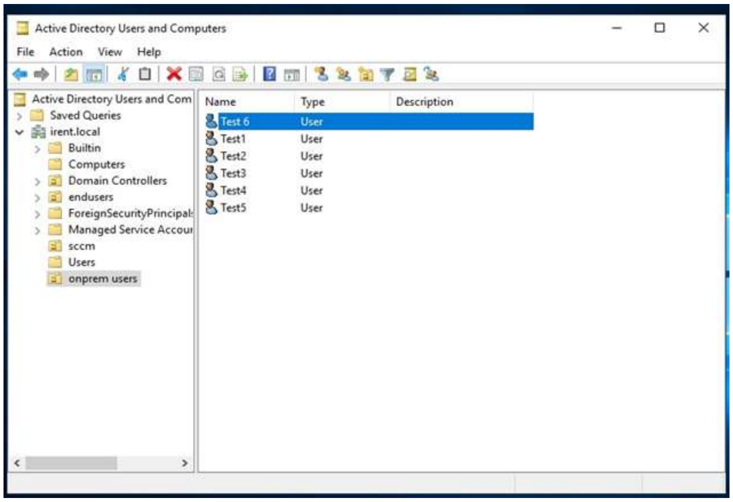


SERVERS
All servers | 1 total

Server Name	IPv4 Address	Manageability	Last Update
DC01	192.168.0.71	Online - Performance counters not started	2/9/2025 11:

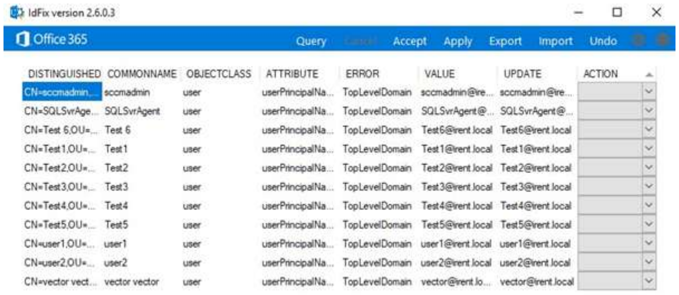
EVENTS
All events | 145 total

Figure 32: AD DS Server



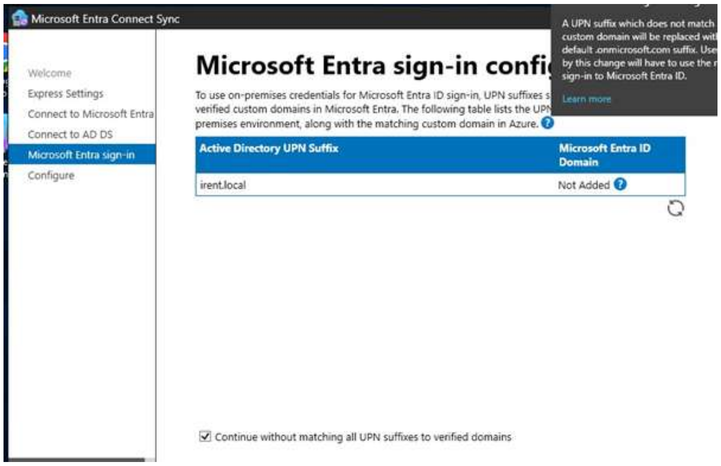
Name	Type	Description
Test 6	User	
Test1	User	
Test2	User	
Test3	User	
Test4	User	
Test5	User	

Figure 33: On prem Users



DISTINGUISHED	COMMONNAME	OBJECTCLASS	ATTRIBUTE	ERROR	VALUE	UPDATE	ACTION
CN=sccmadmin,...	sccmadmin	user	userPrincipalNa...	TopLevelDomain	sccmadmin@ire...	sccmadmin@ire...	
CN=SQLSvrAge...	SQLSvrAgent	user	userPrincipalNa...	TopLevelDomain	SQLSvrAgent@...	SQLSvrAgent@...	
CN=Test 6,OU=...	Test 6	user	userPrincipalNa...	TopLevelDomain	Test6@irent.local	Test6@irent.local	
CN=Test1,OU=...	Test1	user	userPrincipalNa...	TopLevelDomain	Test1@irent.local	Test1@irent.local	
CN=Test2,OU=...	Test2	user	userPrincipalNa...	TopLevelDomain	Test2@irent.local	Test2@irent.local	
CN=Test3,OU=...	Test3	user	userPrincipalNa...	TopLevelDomain	Test3@irent.local	Test3@irent.local	
CN=Test4,OU=...	Test4	user	userPrincipalNa...	TopLevelDomain	Test4@irent.local	Test4@irent.local	
CN=Test5,OU=...	Test5	user	userPrincipalNa...	TopLevelDomain	Test5@irent.local	Test5@irent.local	
CN=user1,OU=...	user1	user	userPrincipalNa...	TopLevelDomain	user1@irent.local	user1@irent.local	
CN=user2,OU=...	user2	user	userPrincipalNa...	TopLevelDomain	user2@irent.local	user2@irent.local	
CN=vector vect...	vector vector	user	userPrincipalNa...	TopLevelDomain	vector@irent.lo...	vector@irent.local	

Figure 34: Microsoft IdFix



Microsoft Entra sign-in confi

To use on-premises credentials for Microsoft Entra ID sign-in, UPN suffixes s
verified custom domains in Microsoft Entra. The following table lists the UPN
premises environment, along with the matching custom domain in Azure.

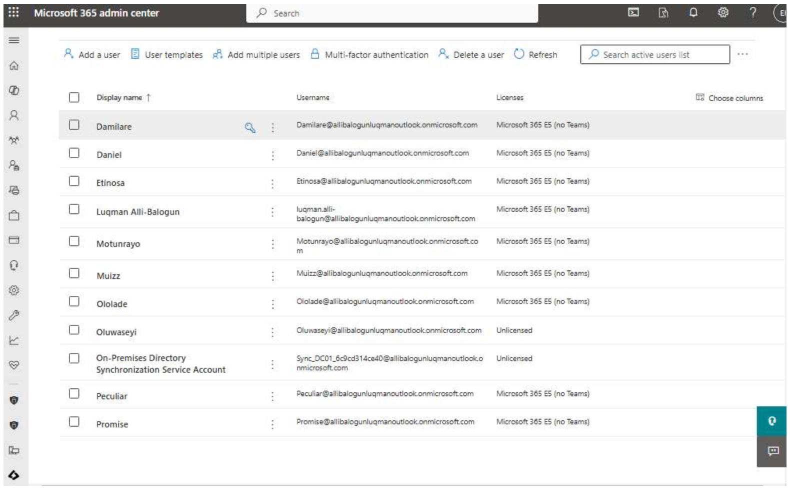
A UPN suffix which does not match
custom domain will be replaced wit
default .onmicrosoft.com suffix. Use
by this change will have to use the r
sign-in to Microsoft Entra ID.

Learn more

Active Directory UPN Suffix	Microsoft Entra ID Domain
irent.local	Not Added

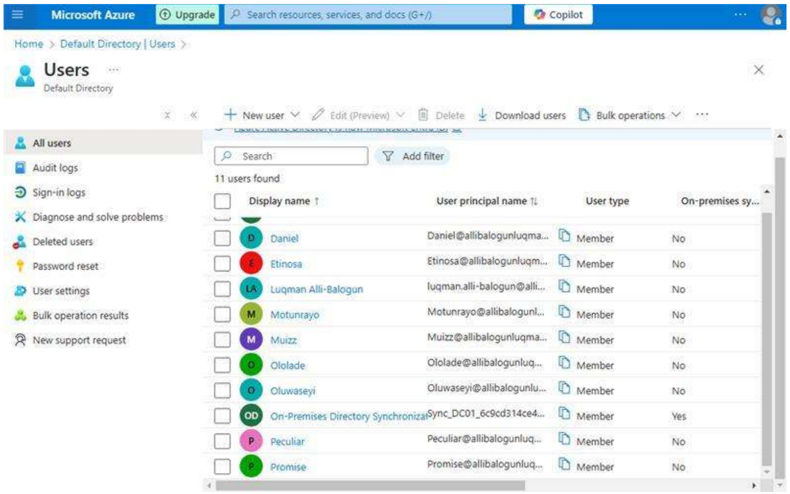
☑ Continue without matching all UPN suffixes to verified domains

Figure 35: Microsoft Entra Directory Sync



Display name ↑	Username	Licenses
Damilare	Damilare@allibalogunluqmanoutlook.onmicrosoft.com	Microsoft 365 E5 (no Teams)
Daniel	Daniel@allibalogunluqmanoutlook.onmicrosoft.com	Microsoft 365 E5 (no Teams)
Etinosa	Etinosa@allibalogunluqmanoutlook.onmicrosoft.com	Microsoft 365 E5 (no Teams)
Luqman Alli-Balogun	luqman.alli-balogun@allibalogunluqmanoutlook.onmicrosoft.com	Microsoft 365 E5 (no Teams)
Motunrayo	Motunrayo@allibalogunluqmanoutlook.onmicrosoft.com	Microsoft 365 E5 (no Teams)
Muizz	Muizz@allibalogunluqmanoutlook.onmicrosoft.com	Microsoft 365 E5 (no Teams)
Ololade	Ololade@allibalogunluqmanoutlook.onmicrosoft.com	Microsoft 365 E5 (no Teams)
Oluwaseyi	Oluwaseyi@allibalogunluqmanoutlook.onmicrosoft.com	Unlicensed
On-Premises Directory Synchronization Service Account	Sync_DC01_6c9cd314ce40@allibalogunluqmanoutlook.onmicrosoft.com	Unlicensed
Peculiar	Peculiar@allibalogunluqmanoutlook.onmicrosoft.com	Microsoft 365 E5 (no Teams)
Promise	Promise@allibalogunluqmanoutlook.onmicrosoft.com	Microsoft 365 E5 (no Teams)

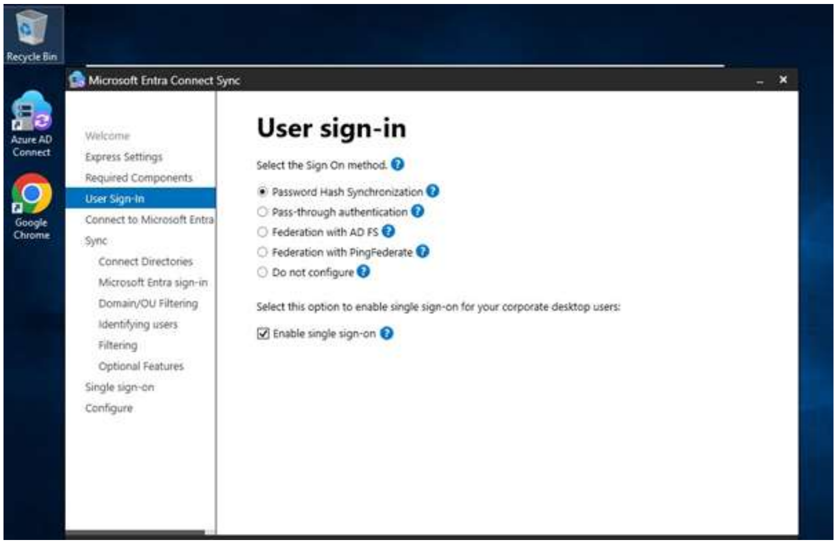
Figure 36: Users before Sync



11 users found

Display name ↑	User principal name ⇅	User type	On-premises sy...
Daniel	Daniel@allibalogunluqma...	Member	No
Etinosa	Etinosa@allibalogunluqm...	Member	No
Luqman Alli-Balogun	luqman.alli-balogun@alli...	Member	No
Motunrayo	Motunrayo@allibalogunl...	Member	No
Muizz	Muizz@allibalogunluqma...	Member	No
Ololade	Ololade@allibalogunluq...	Member	No
Oluwaseyi	Oluwaseyi@allibalogunlu...	Member	No
On-Premises Directory Synchroniza	Sync_DC01_6c9cd314ce4...	Member	Yes
Peculiar	Peculiar@allibalogunluq...	Member	No
Promise	Promise@allibalogunluq...	Member	No

Figure 37: Azure Portal before sync



User sign-in

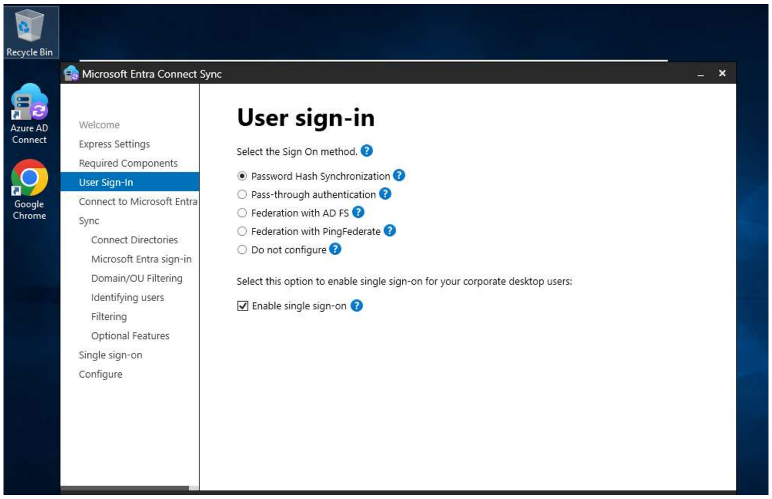
Select the Sign On method.

● Password Hash Synchronization
○ Pass-through authentication
○ Federation with AD FS
○ Federation with PingFederate
○ Do not configure

Select this option to enable single sign-on for your corporate desktop users:

☑ Enable single sign-on

Figure 38: Microsoft Entra Connect Sync



User sign-in

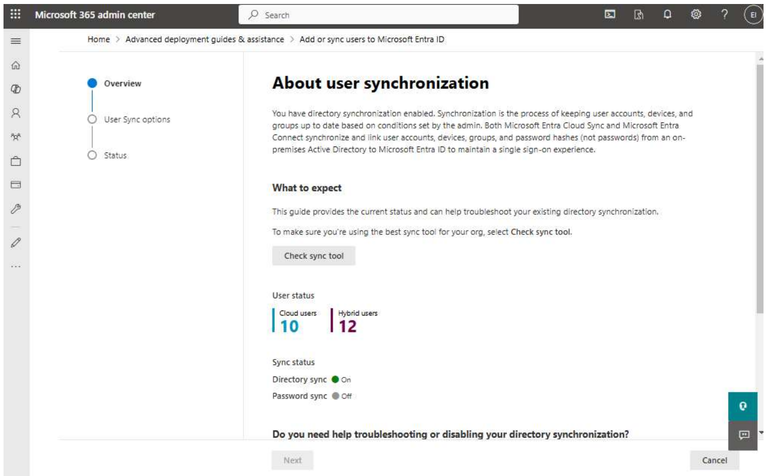
Select the Sign On method.

● Password Hash Synchronization
○ Pass-through authentication
○ Federation with AD FS
○ Federation with PingFederate
○ Do not configure

Select this option to enable single sign-on for your corporate desktop users:

☑ Enable single sign-on

Figure 39: Password hash Synchronization



Microsoft 365 admin center
Search
Home > Advanced deployment guides & assistance > Add or sync users to Microsoft Entra ID
Overview
User Sync options
Status

About user synchronization

You have directory synchronization enabled. Synchronization is the process of keeping user accounts, devices, and groups up to date based on conditions set by the admin. Both Microsoft Entra Cloud Sync and Microsoft Entra Connect synchronize and link user accounts, devices, groups, and password hashes (not passwords) from an on-premises Active Directory to Microsoft Entra ID to maintain a single sign-on experience.

What to expect

This guide provides the current status and can help troubleshoot your existing directory synchronization.

To make sure you're using the best sync tool for your org, select **Check sync tool**.

Check sync tool

User status

Cloud users 10

Hybrid users 12

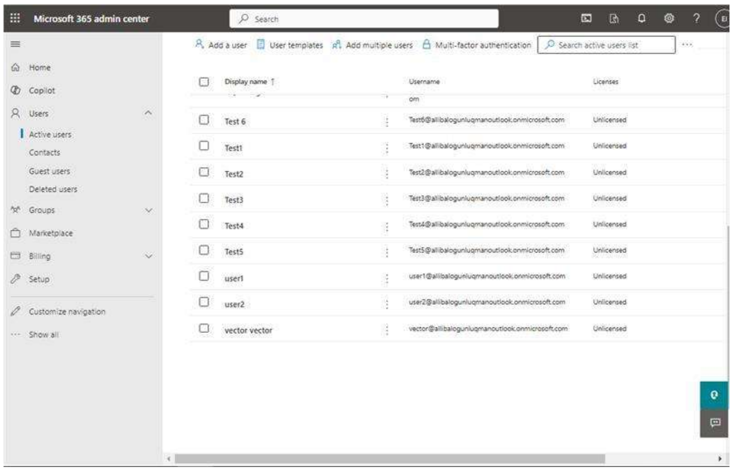
Sync status

Directory sync ● On

Password sync ● Off

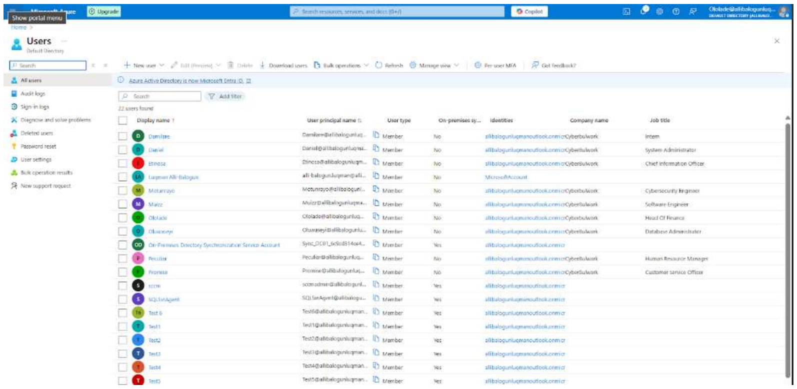
Do you need help troubleshooting or disabling your directory synchronization?

Figure 40: On-prem Synchronization



□	Display name ↑	Username	Licenses
		om	
□	Test 6	Test6@allibalogunluqmanoutlook.onmicrosoft.com	Unlicensed
□	Test1	Test1@allibalogunluqmanoutlook.onmicrosoft.com	Unlicensed
□	Test2	Test2@allibalogunluqmanoutlook.onmicrosoft.com	Unlicensed
□	Test3	Test3@allibalogunluqmanoutlook.onmicrosoft.com	Unlicensed
□	Test4	Test4@allibalogunluqmanoutlook.onmicrosoft.com	Unlicensed
□	Test5	Test5@allibalogunluqmanoutlook.onmicrosoft.com	Unlicensed
□	user1	user1@allibalogunluqmanoutlook.onmicrosoft.com	Unlicensed
□	user2	user2@allibalogunluqmanoutlook.onmicrosoft.com	Unlicensed
□	vector vector	vector@allibalogunluqmanoutlook.onmicrosoft.com	Unlicensed

Figure 41: Users Sync to Cloud



22 users found

Display name	User principal name	User type	On-premises sy...	Identities	Company name	Job title
Damilare	Damilare@allibalogunluq...	Member	No	allibalogunluqmanoutlook.onmicr	Cyberbulwork	Intern
Daniel	Daniel@allibalogunluqma...	Member	No	allibalogunluqmanoutlook.onmicr	Cyberbulwork	System Administrator
Etinosa	Etinosa@allibalogunluqm...	Member	No	allibalogunluqmanoutlook.onmicr	CyberBulwork	Chief Information Officer
Luqman Alli-Balogun	alli-balogun.luqman@alli...	Member	No	MicrosoftAccount		
Motunrayo	Motunrayo@allibalogunl...	Member	No	allibalogunluqmanoutlook.onmicr	Cyberbulwork	Cybersecurity Engineer
Muizz	Muizz@allibalogunluqma...	Member	No	allibalogunluqmanoutlook.onmicr	CyberBulwork	Software Engineer
Ololade	Ololade@allibalogunluq...	Member	No	allibalogunluqmanoutlook.onmicr	Cyberbulwork	Head Of Finance
Oluwaseyi	Oluwaseyi@allibalogunlu...	Member	No	allibalogunluqmanoutlook.onmicr	CyberBulwork	Database Administrator
On-Premises Directory Synchronization Service Account	Sync_DC01_6c9cd314oe4...	Member	Yes	allibalogunluqmanoutlook.onmicr		
Peculiar	Peculiar@allibalogunluq...	Member	No	allibalogunluqmanoutlook.onmicr	CyberBulwork	Human Resource Manager
Promise	Promise@allibalogunluq...	Member	No	allibalogunluqmanoutlook.onmicr	CyberBulwork	Customer service Officer
sccm	sccmadmin@allibalogunl...	Member	Yes	allibalogunluqmanoutlook.onmicr		
SQLSvrAgent	SQLSvrAgent@allibalogu...	Member	Yes	allibalogunluqmanoutlook.onmicr		
Test 6	Test6@allibalogunluqman...	Member	Yes	allibalogunluqmanoutlook.onmicr		
Test1	Test1@allibalogunluqman...	Member	Yes	allibalogunluqmanoutlook.onmicr		
Test2	Test2@allibalogunluqman...	Member	Yes	allibalogunluqmanoutlook.onmicr		
Test3	Test3@allibalogunluqman...	Member	Yes	allibalogunluqmanoutlook.onmicr		
Test4	Test4@allibalogunluqman...	Member	Yes	allibalogunluqmanoutlook.onmicr		
Test5	Test5@allibalogunluqman...	Member	Yes	allibalogunluqmanoutlook.onmicr		

Figure 42: Complete Synchronization

4.6 Challenges Encountered

1. **Initial Synchronization Failures:**
   - We encountered failures due to misconfigurations during the setup process, requiring troubleshooting and adjustments to synchronization settings.
2. **Perceived Synchronization Delays:**
   - We initially believed that users were not syncing and performed multiple synchronization attempts. However, after further troubleshooting, we discovered that synchronization had already occurred, but the changes were not immediately visible.

Results and Findings

1. Achieved seamless identity management across both on-premises and cloud environments.
2. Ensured **consistent user access** to resources with minimal disruptions.
3. Improved monitoring and troubleshooting practices to prevent redundant sync attempts.

Conclusion

In conclusion, the implementation of cloud security solutions, including Microsoft Sentinel for SIEM, Microsoft Purview DLP for data protection, and Azure AD DS for identity management, has significantly enhanced CyberBulwork's security posture. By integrating these tools, we have improved threat detection, incident response, and compliance with data protection regulations.

The process involved configuring Sentinel for threat intelligence, deploying DLP policies to prevent unauthorized data transfers, and synchronizing on-premises Active Directory with Azure AD to streamline identity management. While challenges such as fine-tuning Sentinel, troubleshooting DLP detection issues, and resolving synchronization misconfigurations were encountered, systematic troubleshooting and iterative refinements ensured successful implementation.

Ultimately, these security enhancements have strengthened CyberBulwork's ability to monitor, detect, and respond to security threats, while also ensuring seamless access management and data protection across cloud and on-premises environments.