M365 Tenant Dashboard Technical Guide

March 31, 2025

Envision IT
9-6975 Meadowvale Town Centre Circle
Mississauga ON L5N 2V7
envisionit.com

Table of Contents

Solution Overview

The M365 Tenant Dashboard is a multi-tenant SaaS application created and operated by Envision IT. It consists of the following components:

- .NET 8 application hosted in the Envision IT Microsoft Azure Subscription
- Unique storage accounts for each client for storing the collected data
- Client hosted storage account to ship the Entra ID signin logs to
- Azure Key Vault to hold the access keys for the two storage accounts
- Power BI report that collects and presents the dashboard content

Installation Process

Registration process on https://portal.envisionit.com/

1. Join the https://portal.envisionit.com/members/m365-tenant-dashboard group
    a. Registration of a new account on the portal will be the first step
    b. Join the group
2. Go to the https://portal.envisionit.com/members/m365-tenant-dashboard member page to continue the registration
3. Consent
4. Provide the connection string for the Entra ID sign in log audit storage account

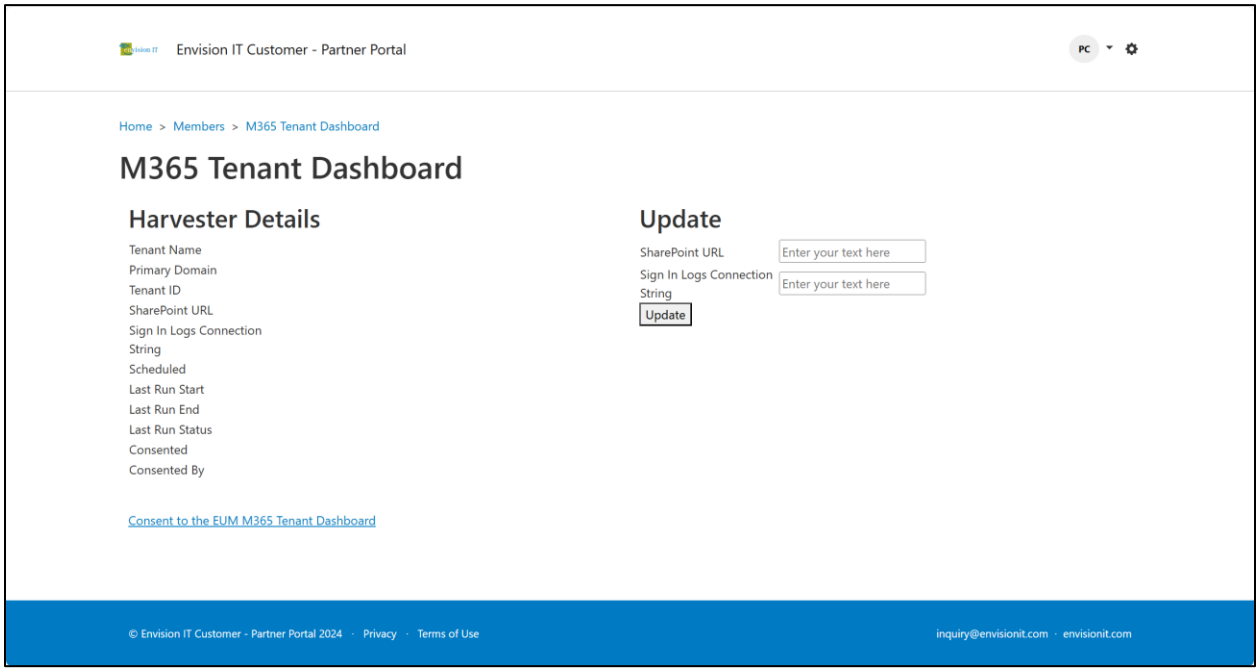
Prerequisites

The following prerequisites are needed prior to commencing the installation.

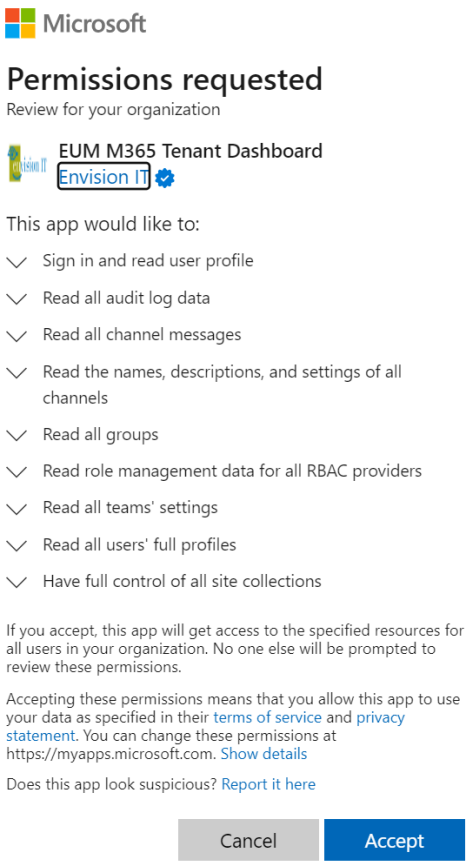
- Entra ID Global Admin account to consent to the app registration
    - Most organizations have elevated accounts for their admin staff separate from their regular working accounts
    - Having the email address of the admin's regular account is fine as the consent can be done under the elevated account
    - If PIM is being used to approve admin account usage, an approved request needs to be submitted prior to starting the installation
- Storage account for Entra ID diagnostic settings audit log shipping
- Paid Azure subscription to host the storage account with Owner or Contributor access

Admin Consent

Reading the structure and configuration of the Microsoft 365 tenant requires the consent of a user with the Global Administrator role. This process begins by signing into M365 Tenant Dashboard | Envision IT Customer - Partner Portal. The Tenant ID is retrieved from the account, and a link is provided to grant consent.



The consent page displays all requested permissions:



Summary of requested permissions:

- Allow authentication to the tenant.
- Provide read access to:
  - Audit log data
  - Teams channel names, descriptions, settings, and messages
  - Groups
  - Read role management data for RBAC providers
  - Teams' settings
  - All users' full profiles
- Provide full control (read/write) access to:
  - SharePoint site collections. This is required to read site settings and policies, including external access properties, permissions. There is no corresponding read-only permission that provides this information.

Reducing App Privileges

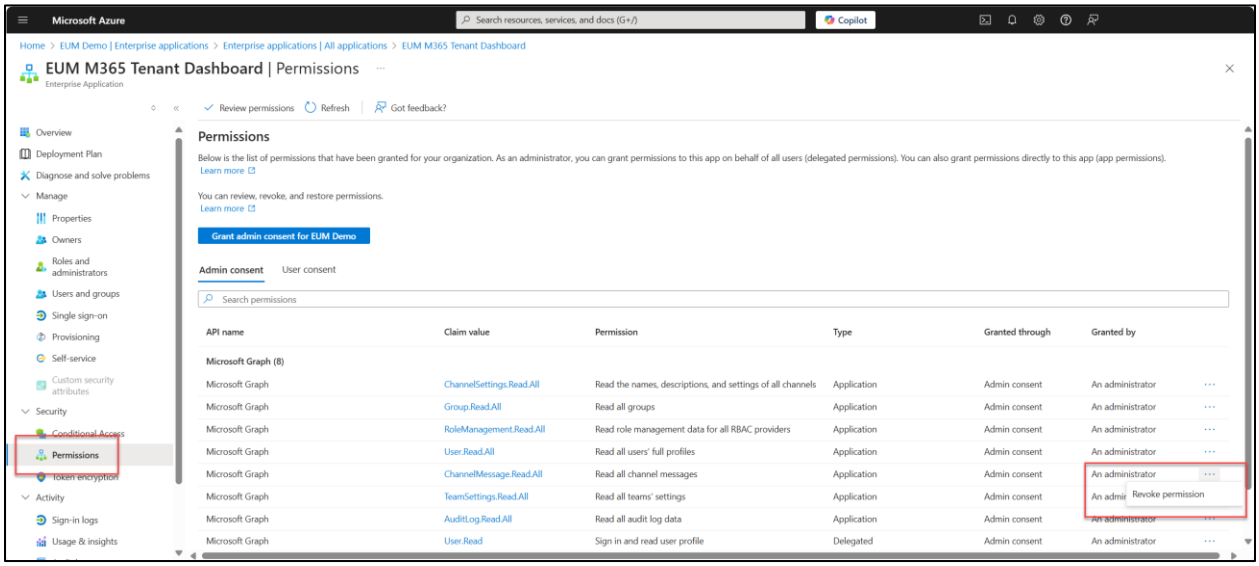
For some clients the above requested permissions are too broad, and a reduced set of permissions is preferred, even though less data will be collected and displayed in the tenant dashboard. The following permissions can be removed once consent is granted. Envision IT will need to be advised so that the data collection can be configured to not include those areas that are no longer permissioned.

- Read all channel messages
- Read the names, descriptions, and settings of all channels
- Read all groups
- Read all teams' settings
- Read all user profiles
- Have full control of all site collections
    - This can be replaced by selected site collections, which requires additional permissioning of the desired site collections, and corresponding configuration of the Data Harvester to have the matching set of site collections

To remove a particular permission follow these steps:

- Open a browser and navigate to [Enterprise applications - Microsoft Azure]
- Search for EUM M365 Tenant Dashboard
- Go to the Permissions tab under Security on the left nav
- On the permission to be removed, use the ellipsis at the end of the selected permission and choose Revoke permission

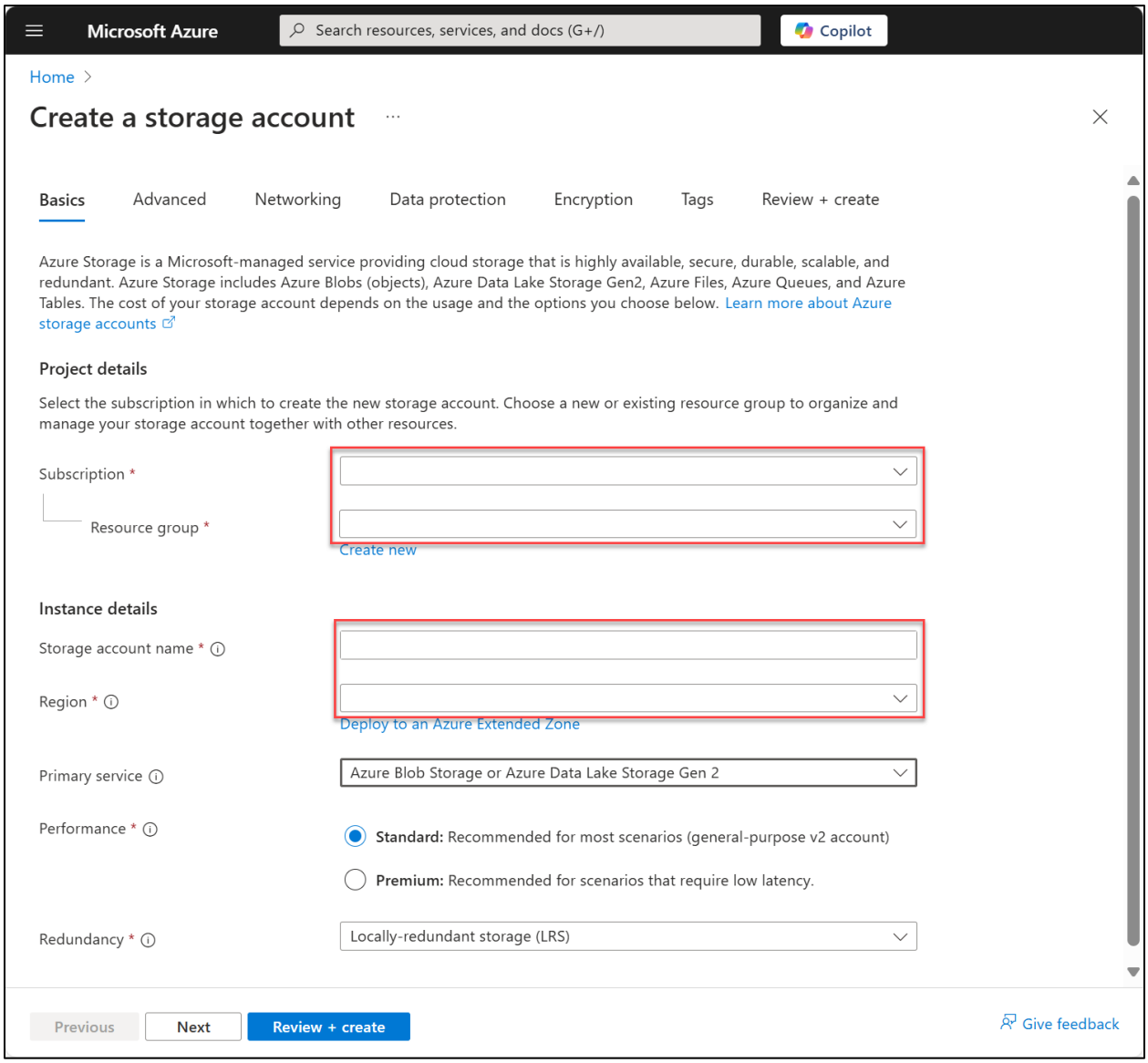
It is important to advise Envision IT on which permissions have been revoked so that the data collection process can be configured appropriately to not request those properties.



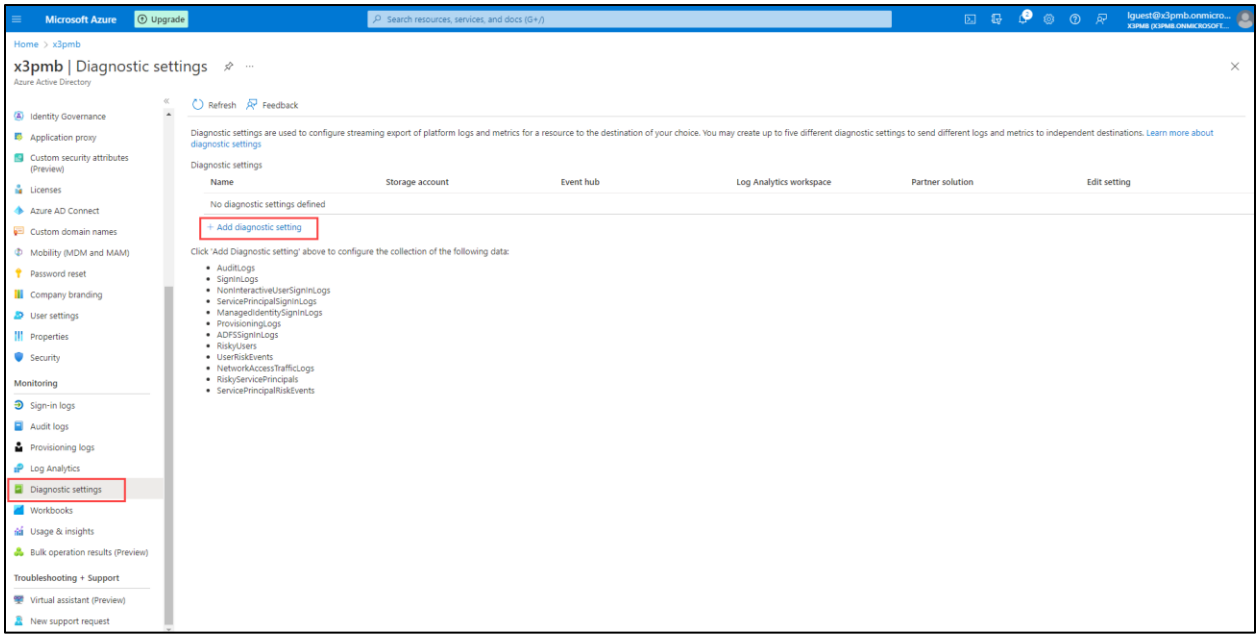
Diagnostic setting for Storage Account

Diagnostic settings are used to configure export of platform logs and metrics for a resource to the storage account. In this case a setting must be created for the Storage Account to define the logs and metrics that need to be collected. A dedicated storage account is recommended for this.

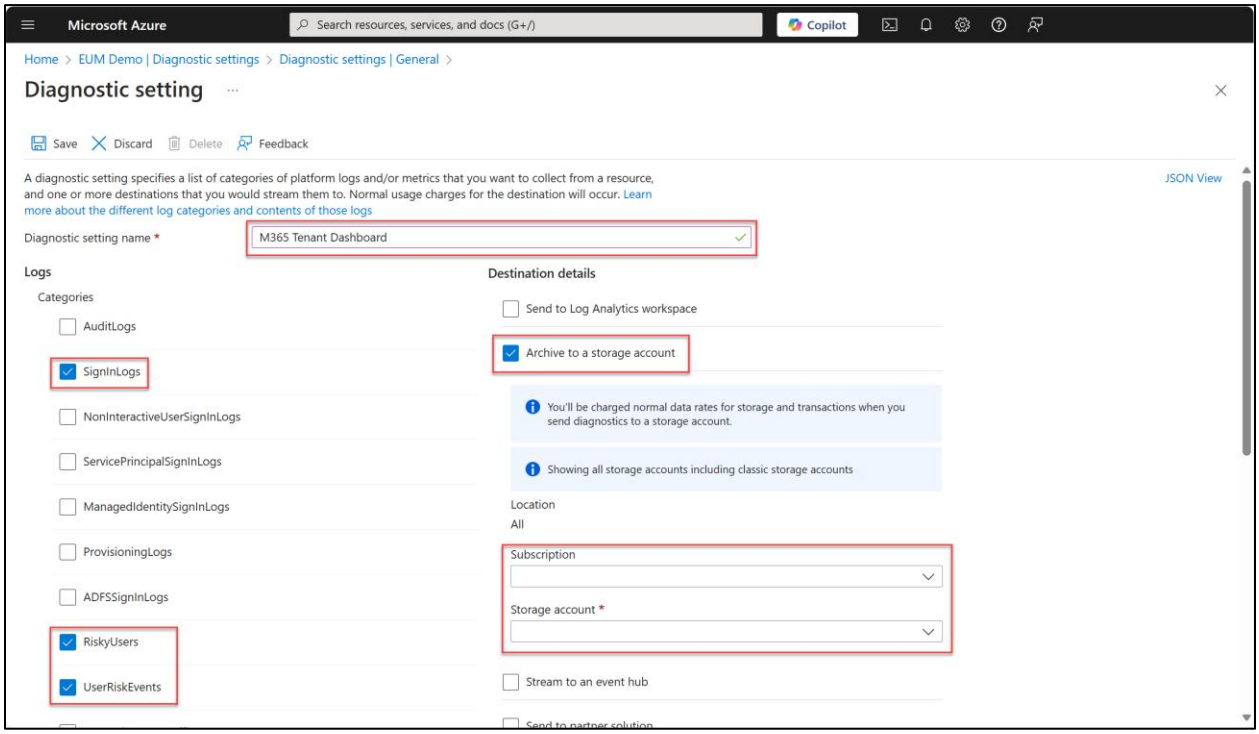
Storage accounts are created in the Azure portal. You will need to specify a paid subscription, resource group, name and region for the storage account. Locally redundant storage is the lowest cost option, and high availability is not a requirement for audit logs.



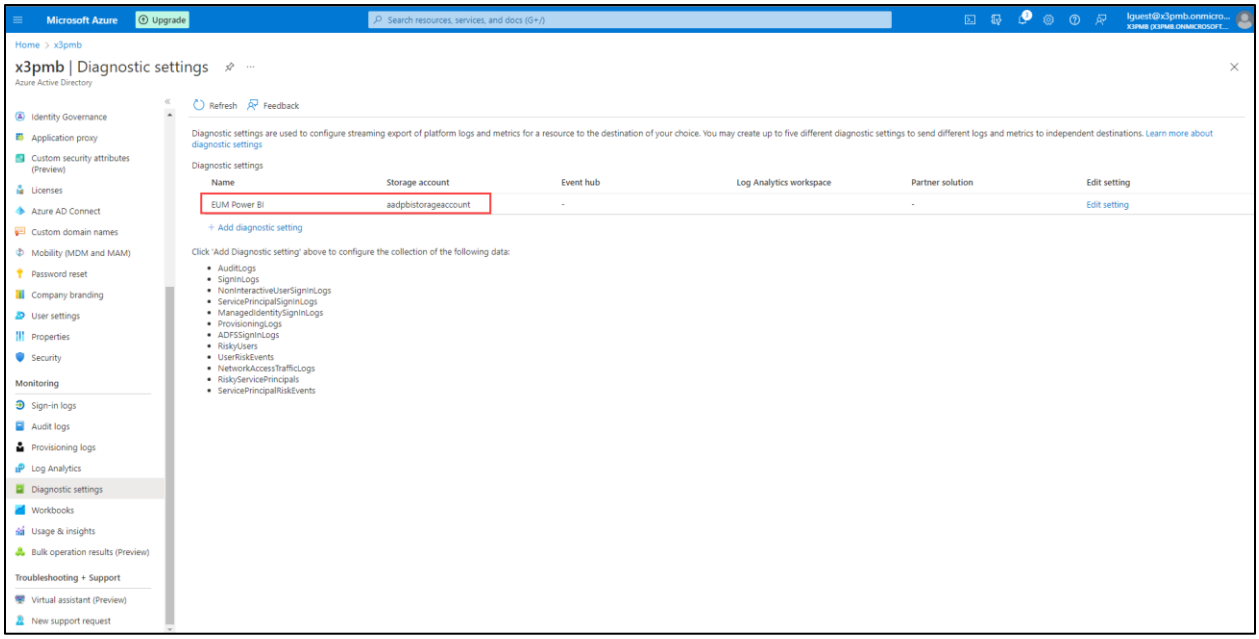
Once the storage account is ready, you can navigate to the diagnostic settings by going to Azure Active Directory and scrolling down to Diagnostic Settings in the left menu under Monitoring.



Set a name for the diagnostic setting, choose Archive to the storage account as the destination and enable the Log categories.



Once you save the diagnostic setting, it will show on the main diagnostic settings page within the Azure portal.



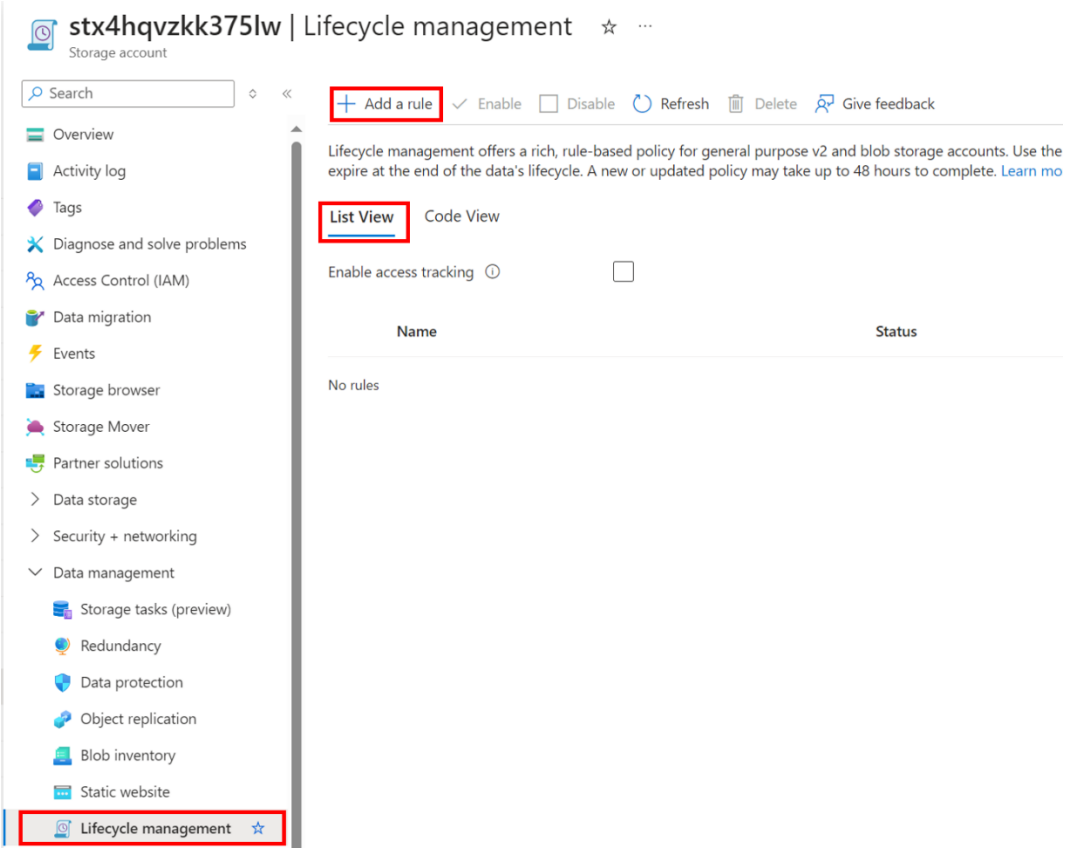
Lifecycle Management for Storage Account

Lifecycle Management is process of managing the data stored in the Storage Account. Here we can setup retention rules to prevent cluttering of the diagnostic settings being archived.

To setup Lifecycle Management, navigate to the storage account you have configured for diagnostic settings.

Under Data management, select Lifecycle Management to view or change lifecycle management policies

Select List View, and select Add a rule

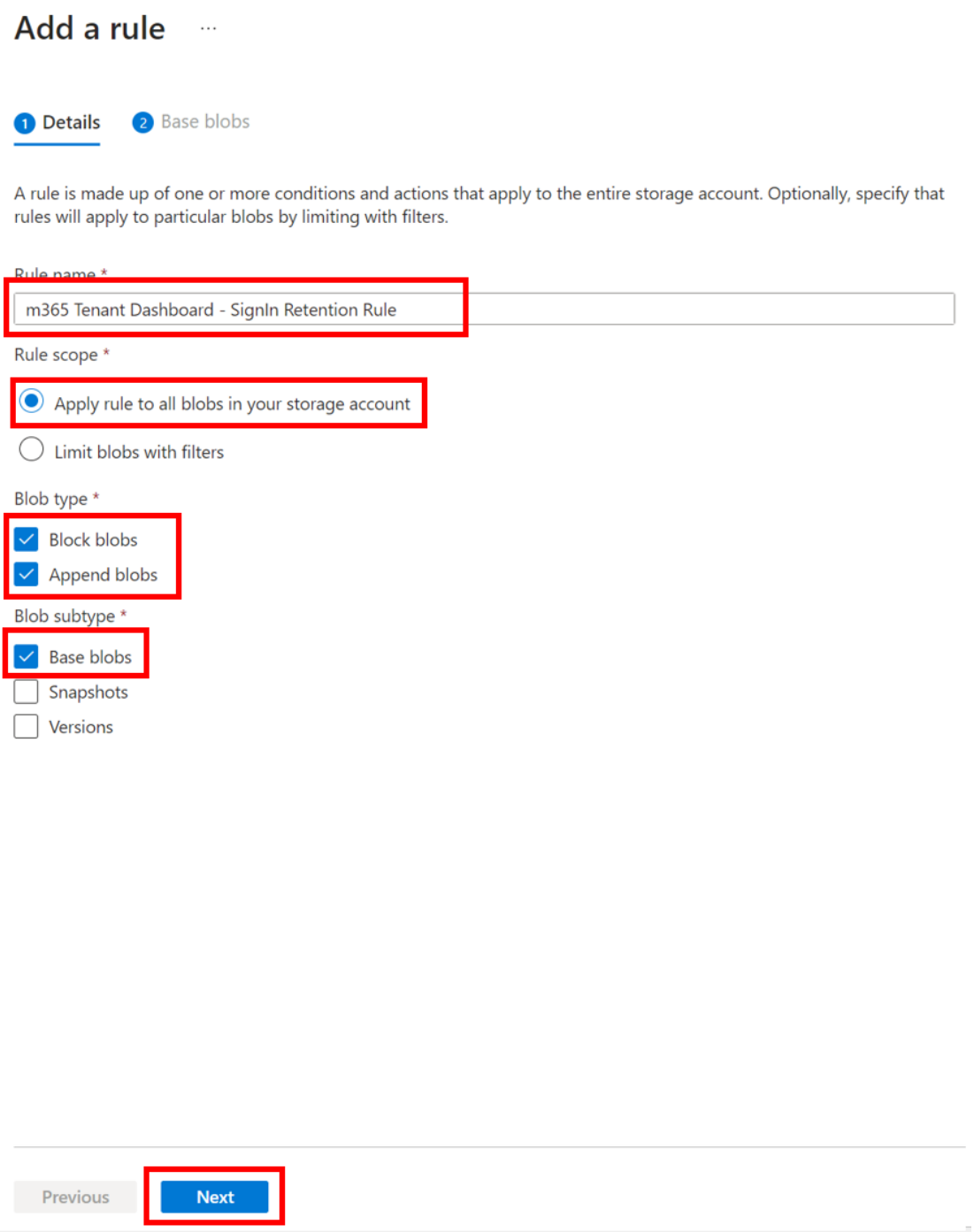


Enter a Rule name

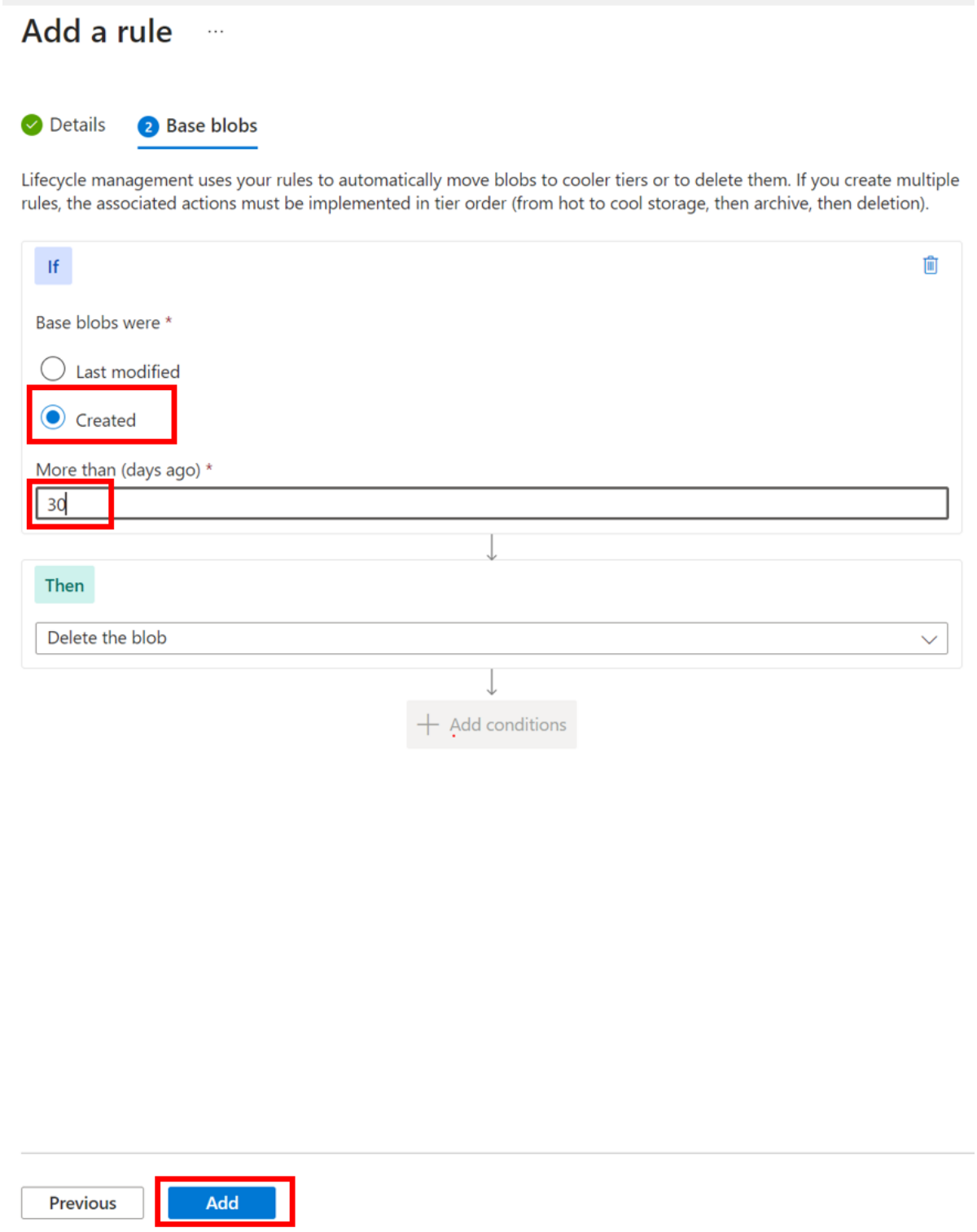
Under Rule Scope, select Limit blobs with filters

Under Blob Type, select Append Blobs and Base blobs under Blob subtype.

Select Next



Set your retention time, then select Add



Reviewing and Refreshing the Dashboard

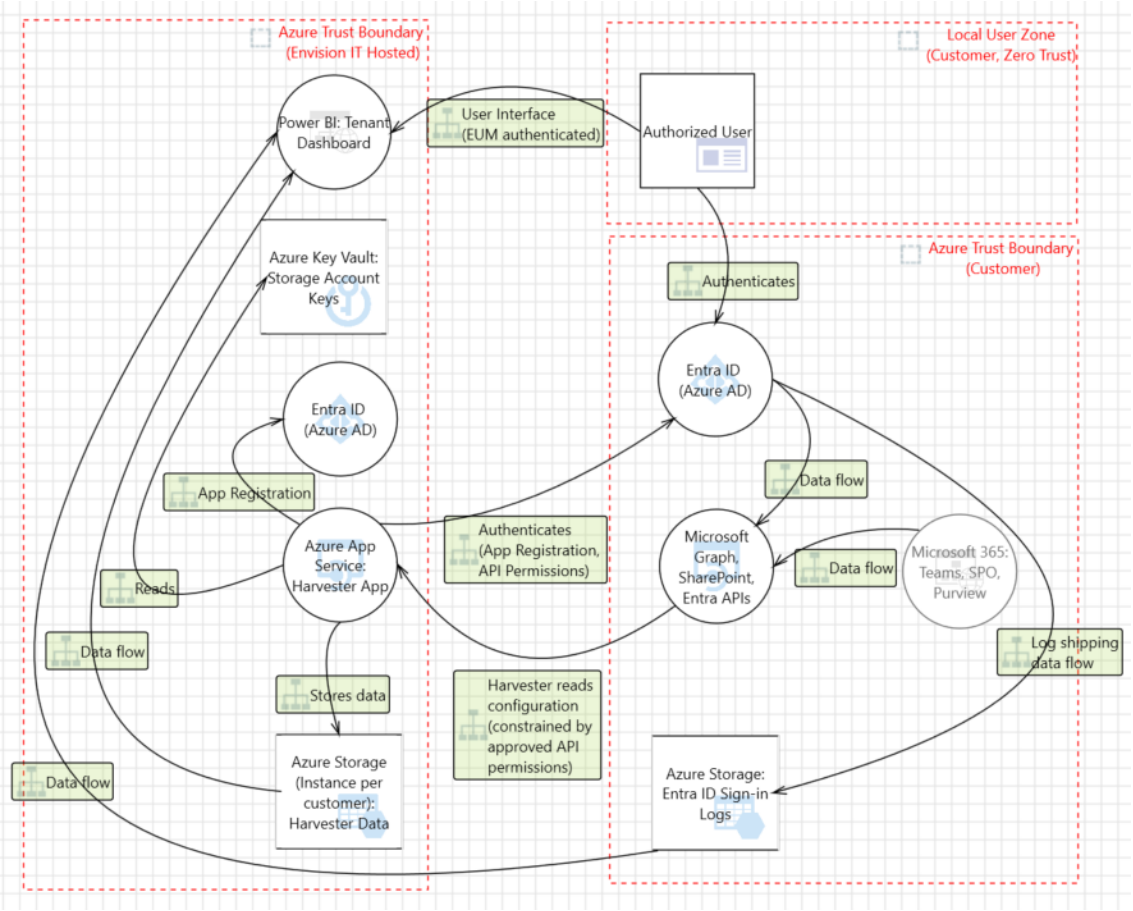
The dashboard is available from the https://portal.envisionit.com/members/m365-tenant-dashboard member page.

Here you can see the following:

- Confirmation that the consent has been granted to run the application
- Last data collection run date and time
- Next scheduled
- Link to the Power BI dashboard
- Link to request a refresh as soon as possible

Appendix A: Tenant Dashboard Architecture

The diagram below describes the components of the Tenant Dashboard including the Harvester application which gathers data from the Microsoft 365 tenant.



Tenant Dashboard Components

Azure Key Vault

- All secrets are stored in an Envision IT Azure Key Vault with security isolation per customer.

Harvester Application

- A multi-tenant Envision IT application.
- Authenticates via an App Registration and Client Secret managed in the Customer's Entra ID directory.
- Performs read-only activities via Customer's Microsoft Graph, SharePoint, Teams, and Entra APIs.
- Permissions requested by the solution are described in

- *Admin* Consent.
    - Permissions are approved in the customer tenant with the Global Admin role (see also:

  - Admin Consent).
  - Read permissions are required to traverse Teams, Sites, and Sign-in Logs.
  - SharePoint Full Control permissions (akin to Site Collection Owner) are required to read ACLs and policies within SPO sites, and external sharing flags.
- Data stores:
  - Envision IT Azure Storage contains an isolated instance per customer for harvested information. Authentication secret held in the Envision IT Azure Key Vault.

Tenant Dashboard Application

- Users authenticate via customer's Entra ID, with dashboard ACLs managed with Envision IT's Extranet User Manager.
- Tenant Dashboard is an EIT Power BI Application.
  - Each customer dashboard is managed in a security-isolated workspace (per customer).
  - Credentials for connected data repositories are stored within Power BI.
- Data sources:
  - Reads tenant data from EIT Azure Storage (isolated per client).
    - Currently an Azure Files File Share. Refreshes happen by updating on Power BI Desktop and saving back to the Power BI workspace.
    - Roadmap: There is a change planned to switch to an Azure Files BLOB store which would support live updating of the dataset from within the dashboard. This would remove the need for manual updates, security boundaries and configuration would otherwise remain the same.
  - Reads last sign-in data from Customer Azure Storage instance. Sign-in Logs are shipped directly from Entra (pipeline has no egress from the customer tenant, requires Entra P1 or P2 license). Authentication secret held in the Envision IT Azure Key Vault instance (per customer).

EIT Azure Storage

- A security-isolated file share instance is created per customer.
- Access keys are stored in an Azure Key Vault, again with an isolated instance per customer.
- Data is solely accessed via dashboard reports, with user access restricted on a need-to-know basis to Envision IT personnel assigned to the customer.
- Data stored:
  - Microsoft 365 Tenant data
    - Microsoft Teams and SharePoint Online (SPO):
      - Teams channels and SPO site collection, site, library, and sub-site data including titles, site and channel types, sensitivity labels.'
      - Groups managing membership and permissions applied, including unique permissions.
      - File data including file types, sizes, counts, and sensitivity labels
      - Last accessed data
      - Not stored:

        - Lists and built-in libraries (site assets, site pages, themes, web parts).
- Entra data
    - User profile data is used in dashboard reports to review permissions granted to active internal and external users.
    - Microsoft 365 Groups including display names, mail-enabled flag, security-enabled flag, group type.