LSEG Workspace | Automated Domain Management (ADM)

Solution Overview (Pilot)

Introduction

This document provides a solution overview for a new LSEG application, the Automated Domain Management (hereafter referred to as ADM) application which assists Microsoft Teams Administrators in keeping their organisation's external collaboration policies in sync with LSEG's Open Directory network of firms.

What is the Automated Domain Management (ADM) app?

The ADM app is a management tool for Microsoft Teams administrators designed to keep external collaboration policies aligned with LSEG's Open Directory network. It automates the process of:

- Subscribing to a domain feed
- Updating federation policies
- Managing collaboration rules at scale

What problem does the ADM app solve?

To communicate externally in Microsoft Teams, organisations must federate with numerous entities in a point-to-point way. Existing workflows require manual processing, which is time-consuming and prone to error. The ADM app automates this process, reduces administrative overhead, and allows policies to remain up to date. ADM features a user-friendly front-end, robust backend services, and is deployed inside the customer's own environment to ensure that sensitive data does not leave the customer data boundary.

How does the app work?

The ADM app creates external access policies within Microsoft Teams, facilitating communication between users and other members of the Open Directory network. These policies, also referred to as external collaboration or federation policies, ensure that only specific individuals in the organisation (in other words, Open Directory users) can communicate only with other Open Directory customers, and to those within your existing federation policies. This capability is enabled by the new Granular Federation Controls feature in Microsoft Teams.

The ADM app will:

- Create new external access policies in Teams
- Synchronise created policies with:
  - Approved domains received from LSEG
  - Other, organisation-managed, policies in Teams
- Assign policies to appropriate users / groups
- Provide workflow for admins to approve / reject domains received from LSEG

The ADM app does not:

- Send tenant configuration or messaging data to LSEG

LSEG DATA & ANALYTICS

- Store tenant configuration other than for policies it manages (which it does locally in your environment)
- Edit existing organisation configuration or policies, except in very limited circumstances and with admin consent (see What is Granular Federation Control?, below).

What is Granular Federation Control?

Granular Federation Control is a new feature in Microsoft Teams which enables administrators to configure different federation policies for different groups of users in their organisation.

For granular federation controls to work, the property AllFederatedUsers must be set to true. This is a tenant-wide setting. The ADM app will check this and inform the administrator that it must be set correctly before continuing. The administrator can do this themselves, or the ADM app can do it on their behalf. Changing this value from false to true will enable federation at the tenant-wide level. If this was set to prevent any federation within the tenant, the admin should set the AllowedDomains property to null.

For more information, see Set Tenant Federation Configuration and Set External Access Policy on Microsoft Learn.

How does the ADM app know which settings and domains to configure?

New policies generated by the ADM app are based upon a pre-existing policy that is managed by the organisation's administrator within the Teams Admin Centre (TAC). The ADM app continuously synchronises these new policies with the corresponding base policy. Administrators continue to update their org policies as usual, and the ADM app keeps the policies it manages aligned with any updates made by administrators to the base policy in the TAC.

Federated domains are configured on the ADM-managed policy by referencing both the original baseline policy and the list of approved domains provided by LSEG. This approach allows approved domains from LSEG to be configured, while retaining the organisation’s ability to customise policies enabling communication beyond Open Directory.

ADM does not edit any organisation-managed policies, meaning that administrators can continue to manage their existing policies as usual and the ADM app will resolve any policy conflicts as per the settings chosen by the administrator.

How does the ADM app know which users should be assigned the policy?

The app knows which users should be assigned the policy once administrators have created the relevant security groups and specified users to them.

Do I have control over these policies?

Yes. Administrators can specify whether new domains added to the network by LSEG should be automatically approved and applied to their organisation’s policies, or if approval is required first.

Additionally, administrators can specify ’always-block‘ lists that take precedence over the domain feed, ensuring critical domains remain blocked regardless of feed updates.

As policies are synced with base organisation policies, administrators continue to manage their organisation policies as usual, and changes will be replicated to the corresponding ADM-managed policy. This allows administrators to add additional domains which are not members of Open Directory, ensuring users are still able to communicate with these organisations.

How does the ADM app handle security and compliance?

The ADM app leverages Microsoft Azure’s platform-managed services to allow high availability, security, and compliance. It supports secure authentication with Entra ID and maintains comprehensive audit logs. The ADM app requires a service principal in your Entra tenant so that it can connect to the Teams PowerShell service. This service principal requires the Teams Administrator privileges.

The ADM app also requires administrators to create an app registration in Entra to enable SSO to the management portal.

What technology does this use and how is it deployed?

The solution uses Azure platform-managed services, which provide native high availability without requiring custom application-level high availability logic.

The ADM app will have dependencies on the following Azure platform services:

- Azure Container Apps
- Azure Static Web Apps
- Key Vault
- Application Insights
- PostgreSQL

Services such as Azure App Service, Function Apps, Key Vault, and Entra ID are inherently resilient and distributed, ensuring uptime through zone and regional redundancy.

For disaster recovery, the solution is designed to be re-deployable by administrators in alignment with their specific disaster recovery requirements. Infrastructure-as-Code templates support rapid provisioning in alternate regions, while data services use geo-redundant configurations to protect against regional failures. Key Vault secrets and configuration settings can be replicated across vaults, and monitoring via Application Insights allows visibility and supports proactive recovery actions.

Deploying the ADM app requires provisioning infrastructure in Azure, which can be automated using Azure Resource Manager (ARM) and PowerShell deployment scripts.

Customers are free to tailor the solution per their requirements, for example selecting alternative high availability / disaster recovery options, scaling, network connectivity, load balancing, and so on.

Features

Domain feed subscription

Support subscribing to an external domain feed source *(confidential, patent pending)* to receive updates on domains which are added to and removed from the Open Directory network. This service is hosted in LSEG infrastructure, exposed to customers via a REST API. This feed source will:

- Provide a complete list of network member domains
- Authenticate API requests using a secret key

Update approval workflow

Changes, such as domain additions or removals, or changes to policy assignments, can be flagged for admin approval before deployment.

Always-block lists

Administrators can specify domains that are always blocked, overriding domain feed data. Will not be supported in ADM for the Pilot, but can be handled via Teams Admin Center leveraging Granular Controls capability. This feature will become available for GA.

Teams policy management

The ADM app will create and manage Teams federation policies for Open Directory users and will keep these policies in sync with the domain feed and other existing organisational policies.

Audit logging

Comprehensive logging of all changes, approvals, and user actions made within the app. Logs are written to PostgreSQL, from which the customer can import into other platforms as they require. In addition, Microsoft Purview audit logs contain details of any changes made to the M365 tenant, including changes made by ADM app.

Customer telemetry

The ADM app will integrate with Azure App Insights to provide customer administrators with necessary information to monitor health and status of the application

LSEG telemetry

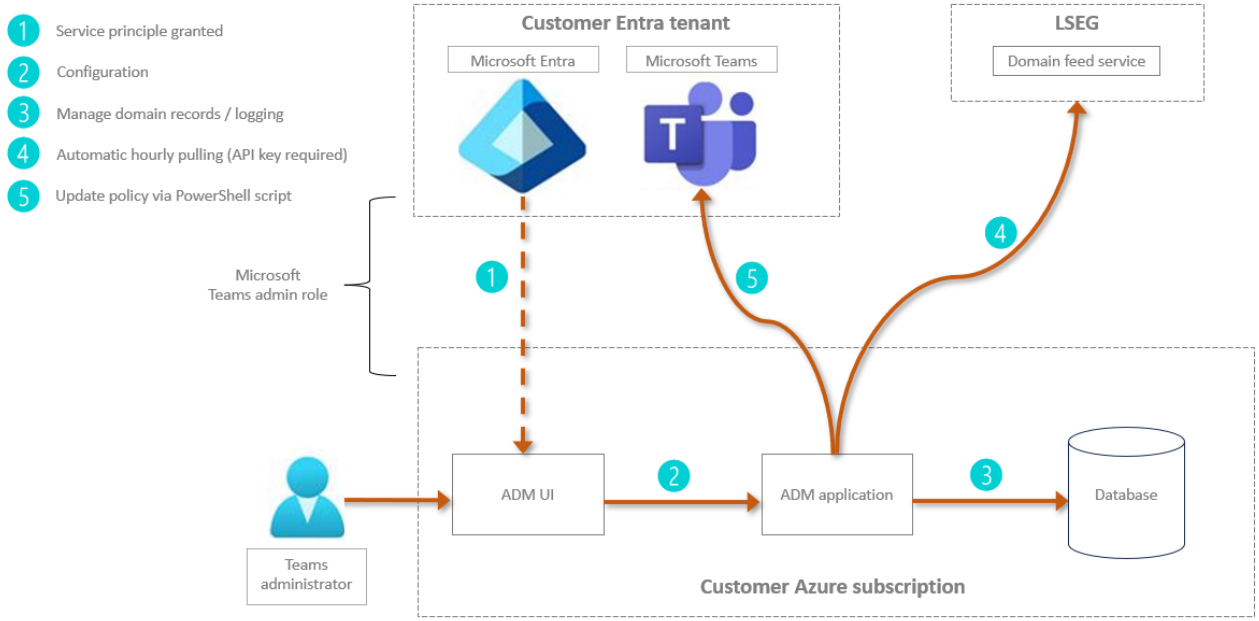
The ADM app will not provide explicit telemetry signals to LSEG, although LSEG will be able to infer when a client last checked in to the API and therefore the latest version of the domain list they have received.

Authentication and authorisation

The app will integrate with Entra ID for secure user and app authentication.

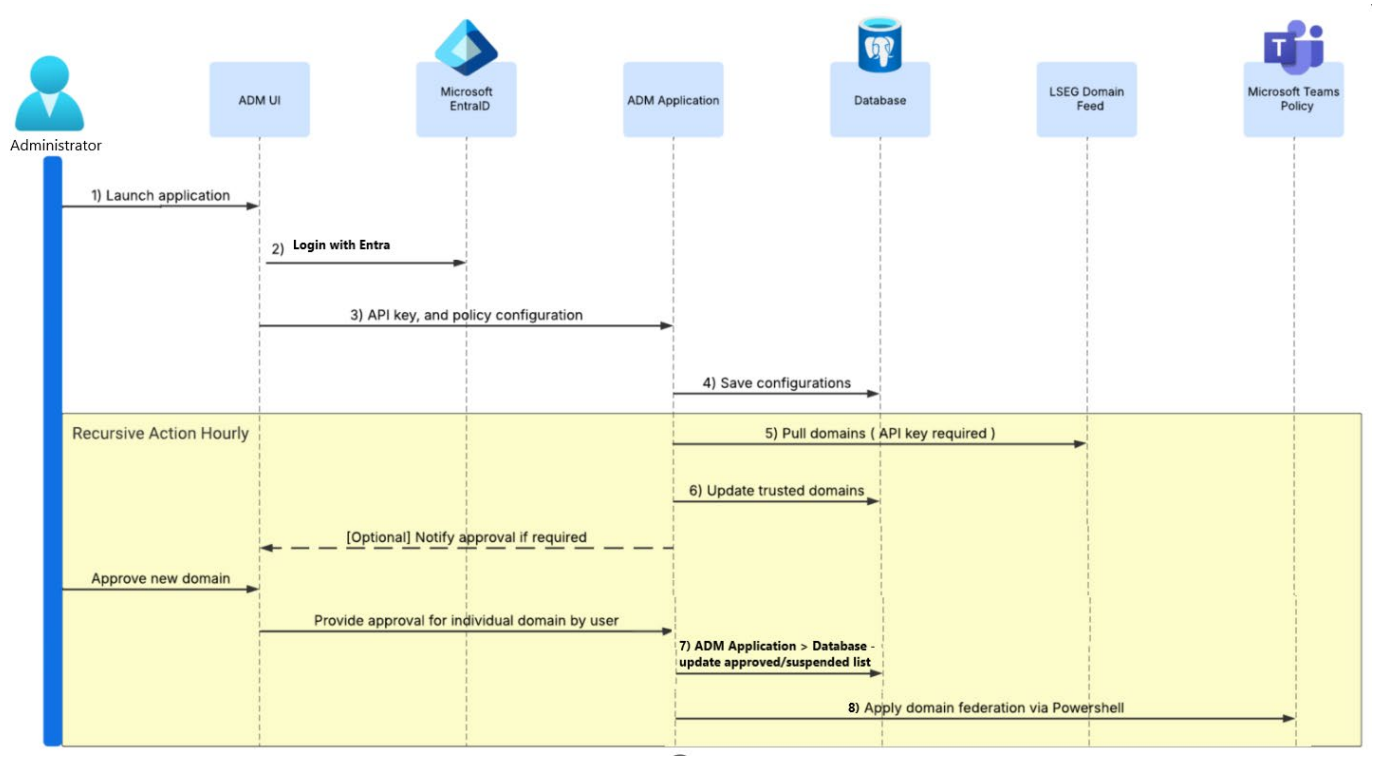
Architecture

Automated Domain Management (ADM) application architecture diagram:



Sequence of events

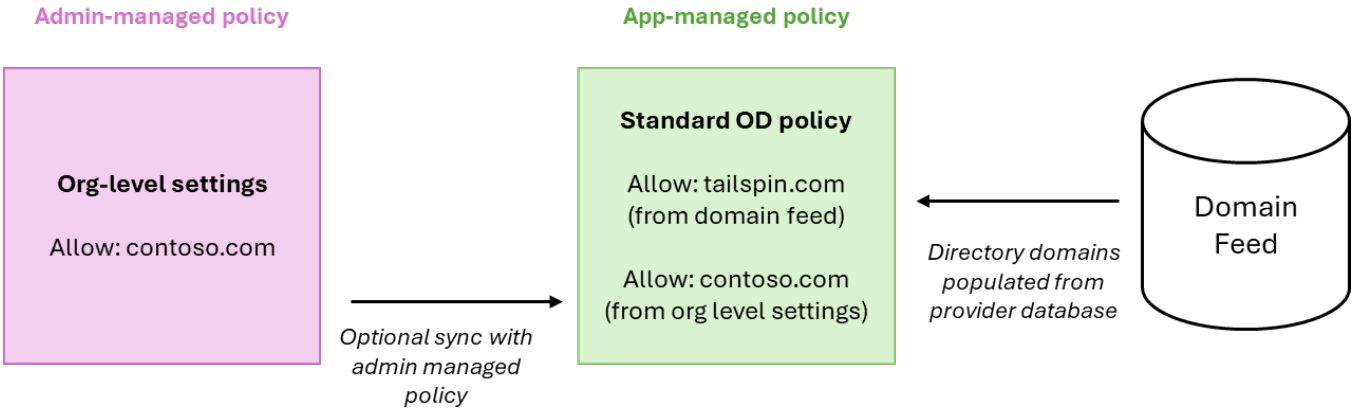
Automated Domain Management (ADM) sequence of events diagram:



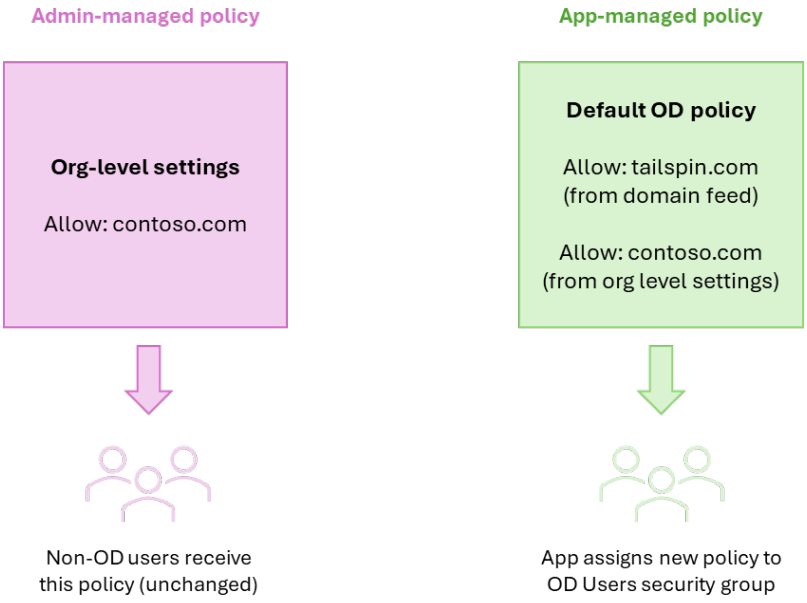
MSFT Teams external federation policy management with the ADM app

The following section demonstrates worked examples of the process flow, with expected outcomes.

Example 1: Create a new standard Open Directory policy

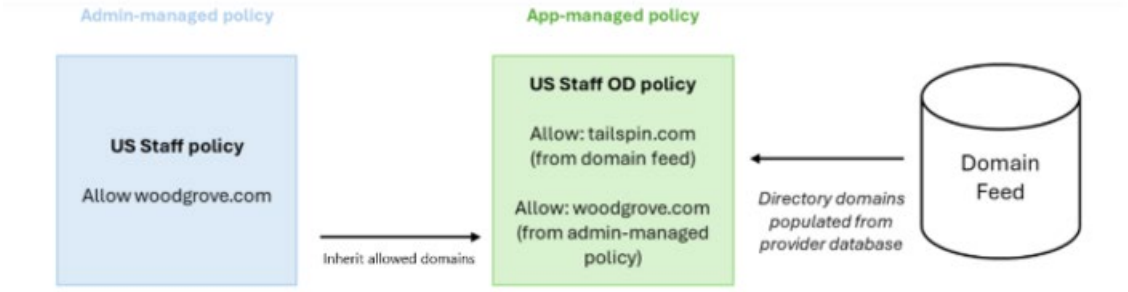


Example 2: Assign new standard policy to Open Directory users

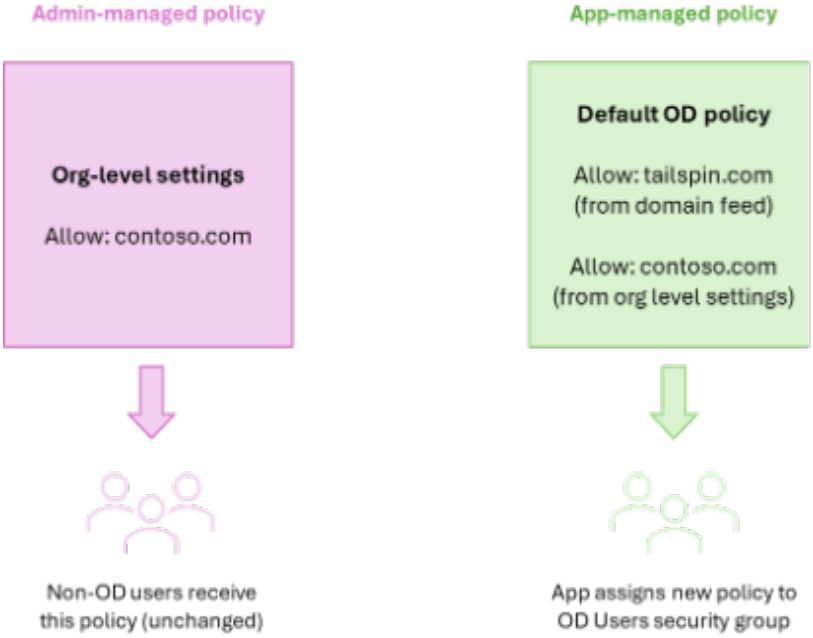


Example 3: Create additional Open Directory policies

Where an organisation has additional external collaboration policies already, and these existing policies apply to users who need to use Open Directory, the ADM app will need to maintain multiple Open Directory policies.



Example 4: Assign additional Open Directory policies to users



Legal information

lseg.com

LSEG DATA & ANALYTICS

Document version: 100.01