



Support Access Policy

e: info@redactxpert.ai

w: <https://www.redactxpert.ai>

Powered by Simpson Associates



Contents

- 1. Introduction..... 3
 - 1.1 Purpose 3
 - 1.2 Scope..... 3
- 2. Guiding Principles 3
- 3. Identity and Access Management 4
 - 3.1 PIM Activation Requirements 4
 - 3.1.1 Justification..... 4
 - 3.1.2 Support Ticket..... 4
 - 3.1.3 Maximum Activation Time..... 4
 - 3.1.4 Approvals 4
- 4. Support Access Process 5
- 5. Support Audit Process 8

1. Introduction

1.1 Purpose

This policy defines how support and service desk users access the RedactXpert multi-tenanted SaaS platform to perform support activities. This includes the process for accessing customer (tenant) infrastructure and data stores.

Its purpose is to document how support staff can perform controlled, auditable support activities, whilst ensuring customer data confidentiality, integrity, and availability.

1.2 Scope

This policy applies to:

- All RedactXpert support and service desk personnel
- All customer tenants hosted within the RedactXpert platform
- All access to Azure platform resources and customer data stores, including SQL databases and Blob Storage

2. Guiding Principles

- **Least Privilege:** Access is granted only when required and only to the minimum level necessary.
- **Just-In-Time Access:** All privileged access is time-bound and approval-based.
- **Separation of Duties:** No individual can both request and approve privileged access for themselves.
- **Data Plane Protection:** Administrative access does not imply access to customer data.
- **Sensitive Data Protection:** RedactXpert staff cannot access documents uploaded by users, their contents, or sensitive metadata such as the PII detected.
- **Auditability:** All access is logged, reviewed, and traceable.

3. Identity and Access Management

RedactXpert uses Microsoft Entra Privileged Identity Management (PIM) to manage all privileged access to the platform, including customer infrastructure and data.

The following characteristics apply:

- All elevated access is inactive by default
- Access requires explicit activation
- Activation requires justification and, for privileged access, approval
- Access is time-limited
- All activities are logged and auditable

3.1 PIM Activation Requirements

As standard, all support activities involve activating relevant PIM roles to be able to gain access to parts of the system.

3.1.1 Justification

All PIM role activations must include a justification from the user as to why the access is required for audit purposes.

3.1.2 Support Ticket

For most PIM activations, details of the support ticket must be provided so that the activation can be traced back to a relevant support activity. This can either be a JIRA support ticket, or a DevOps support ticket depending on the type of activity being performed, and where the details are being tracked.

3.1.3 Maximum Activation Time

All PIM role activations for support access to both the platform and data planes have a maximum allowable time of 4 hours.

3.1.4 Approvals

Depending on the type of PIM role being activated and the level of access it grants, approvals may be required. For privileged access (such as accessing metadata around customer redaction requests), approvals are always required.

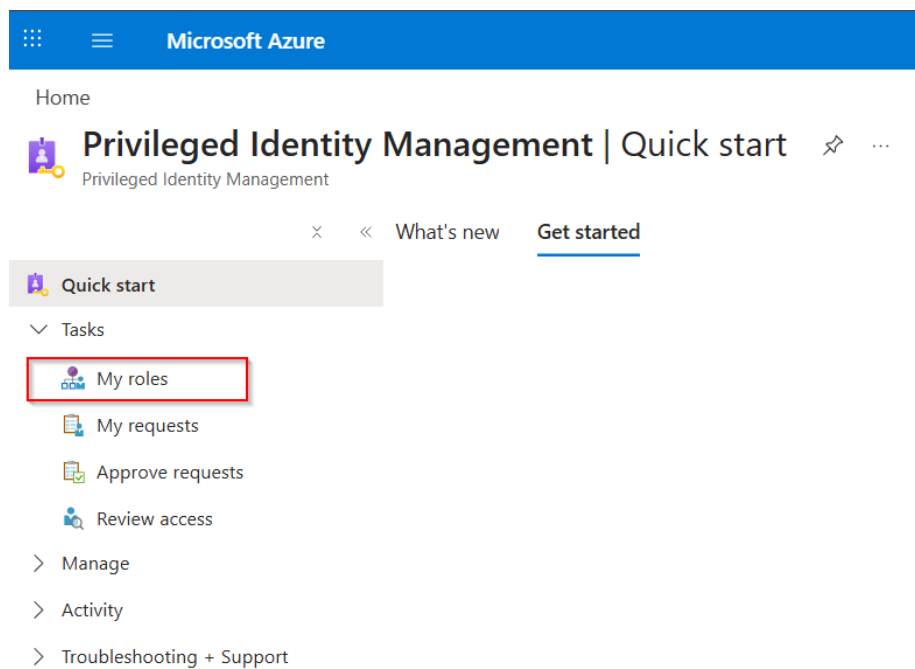
Where an approval is needed, it must be approved by another member of the team (i.e. self-approval is not allowed).

4. Support Access Process

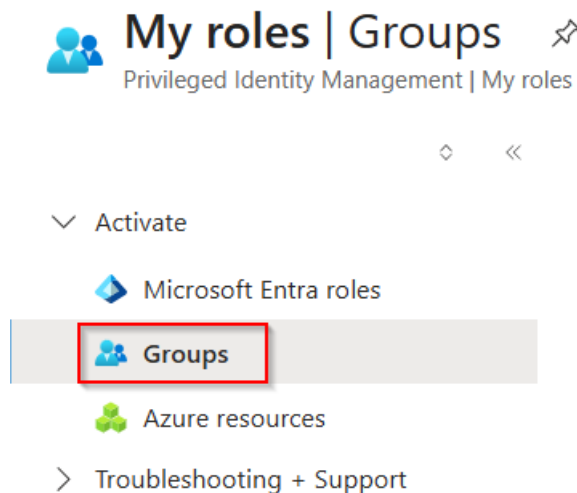
The following steps outline the process for a member of the RedactXpert support team to gain access to the solution for troubleshooting/maintenance tasks.

Note that this does not include the process for gaining access as part of break glass accounts in the case of emergencies (this is documented separately).

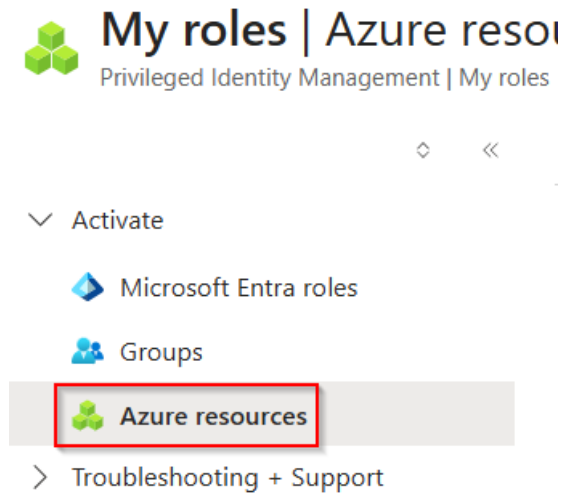
1. Login to the RedactXpert Azure tenant
2. Go to Privileged Identity Management (PIM)
3. Select **My roles** from the left-hand menu



4. Select the relevant PIM role type depending on what you require access to.
 - a. If you require access to the data-plane as part of the support activity, select **Groups**



- b. If you require access to the platform control-plane as part of the support activity, select **Azure resources**



5. Under **Eligible Assignments**, find the relevant group/role that gives the permissions you require, then select **Activate** next to that row

Eligible assignments					
Active assignments					
Expired assignments					
Search by role or group					
Role	Group	Group type	Membership	End time	Action
Member		Security	Group	Permanent	Activate
Member		Security	Group	Permanent	Activate
Member		Security	Group	Permanent	Activate
Member		Security	Group	Permanent	Activate
Member		Security	Group	Permanent	Activate
Member		Security	Group	Permanent	Activate
Member		Security	Group	Permanent	Activate
Member		Security	Group	Permanent	Activate
Member		Security	Group	Permanent	Activate
Member		Security	Group	Permanent	Activate
Member		Security	Group	Permanent	Activate

6. In the blade that appears, enter the required information, then select **Activate**:
 - a. Choose a suitable length of time to have the role enabled (maximum of 4 hours)
 - b. Enter a justification/reason for why you require the role
 - c. For activation of some roles, a ticket number is required, along with the ticket system

Activate - Member

Privileged Identity Management | Groups

Roles

Activate

Status

☐ Custom activation start time

Duration (hours)

①

4

Ticket system

DevOps

✓

Ticket number *

7078

✓

Reason (max 500 characters) * ①

Example

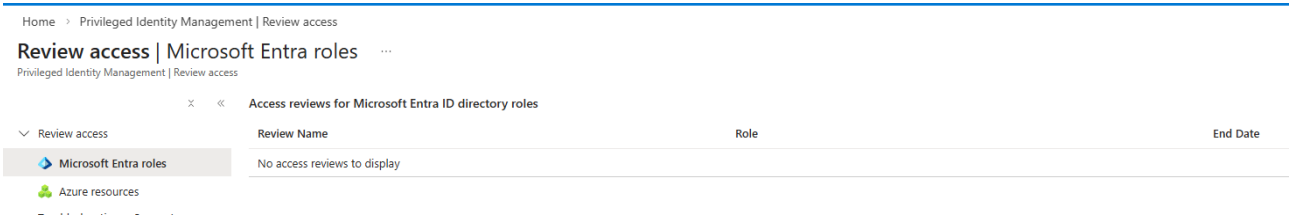
Activate

- The role will then be activated (this may take a few minutes). In some cases, you may also need activation to be approved by another member of the team.

5. Support Audit Process

The following steps outline the process for a member of the RedactXpert support team to gain access to the PIM Audit logs to provide records of what privilege escalations have been requested and approved.

- 1. Login to the RedactXpert Azure tenant
- 2. Go to Privileged Identity Management (PIM)
- 3. Select Review Access from the Tasks menu in the navigation pane
- 4. Select to review either Entra Id Role Assignment or Azure Resources



Note: Data omitted from the screenshot as it would disclose admin user accounts and resource names