





Protect Your Conditional Access Policies

Pro-Vision.IO Inc.

Why CA Gatekeeper?

- **Multi-tenant** support for Conditional Access (CA) policies
- **Prevent** changes to existing policies  **protected**
- **Approval workflow** for changes in policies  **managed**
- **Restore** policies to a specific change/date & time
- **Free text search** – e.g., application or user listed in policies
- **Friendly view** of policy settings
- **Friendly view** of changes in policies
- **Disable or Restore ALL** policies, in case of a crisis (Panic button)
- **Granular management** capabilities
- **Break glass accounts** insights

CA Gatekeeper Portal



All Tenants Dayone App Pro-vision Blue XYZ **Efi Demo Tenant**

Include Non-Interactive Sign-ins

Last 24 Hours Last 7 Days Last 30 Days **Lifetime**

Total Number of Policies

5

Number of Policy Changes

10

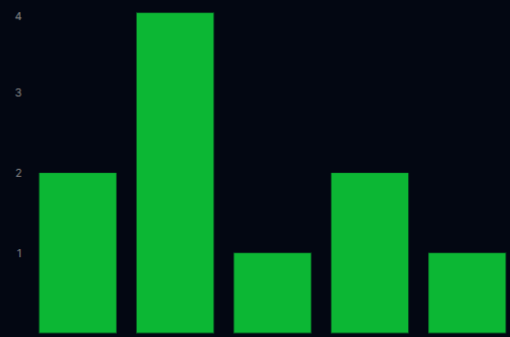
Access Granted Without Policy

8

Application Access Granted Without Policy

2

Changes In Policies



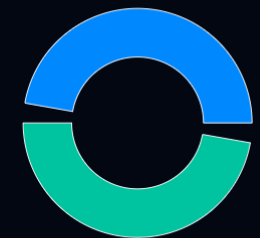
Last updated 6/6/2024, 9:20:10 AM

Access Granted Without Policy



Last updated 6/6/2024, 9:20:10 AM

Application Access Granted Without Policy



● Azure Portal ● Microsoft Graph Command Line Tools

Last updated 6/6/2024, 9:20:10 AM

Entra ID Conditional Access View changes

Home > Conditional Access

Conditional Access | Audit logs

- Overview
- Policies
- Insights and reporting
- Diagnose and solve problems
- Manage
- Monitoring
 - Sign-in logs
 - Audit logs**
- Troubleshooting + Support

Download Export Data Settings Refresh Columns Got feedback

This view will soon be replaced with a view that includes custom security attribute logs, infinite scroll

Date: Last 24 hours Show dates as: Local Service: All Category: All

Date	Service	Category	Activity
6/6/2024, 9:13:50 AM	B2C	Authentication	Validat
6/5/2024, 6:21:22 PM	Conditional Access	Policy	Update
6/5/2024, 6:21:22 PM	Core Directory	Policy	Update
6/5/2024, 6:21:22 PM	Core Directory	Policy	Update
6/5/2024, 6:21:07 PM	Conditional Access	Policy	Update
6/5/2024, 6:21:07 PM	Core Directory	Policy	Update
6/5/2024, 6:21:07 PM	Core Directory	Policy	Update
6/5/2024, 6:19:18 PM	Conditional Access	Policy	Add cc
6/5/2024, 6:19:18 PM	Core Directory	Policy	Update
6/5/2024, 6:19:17 PM	Core Directory	Policy	Add pe
6/5/2024, 6:15:13 PM	Conditional Access	Policy	Update
6/5/2024, 6:15:13 PM	Core Directory	Policy	Update
6/5/2024, 6:15:12 PM	Core Directory	Policy	Update

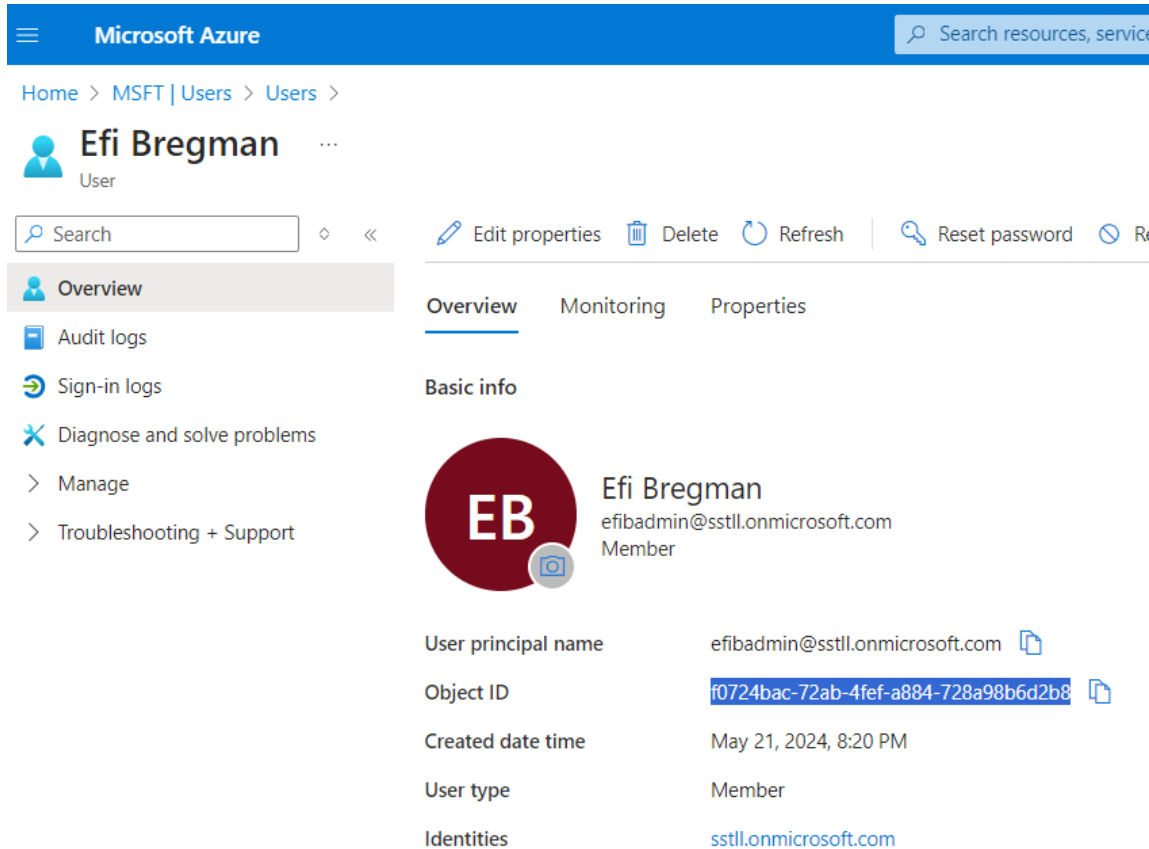
Conditional Access policy changes

This editor feature is currently in (Preview).

Side-by-Side

```
1 {
2   "id": "27c4a5ac-5cf6-40
3   "templateId": "a3d0a415
4   "displayName": "Require
5   "createdDateTime": "202
6   "state": "enabled",
7   "conditions": {
8     "applications": {
9       "includeApplica
10      "All"
11    },
12    "excludeApplica
13    "includeUserAct
14    "includeAuthent
15    "applicationFil
16  },
17  "users": {
18    "includeUsers":
19    "All"
20  },
21  "excludeUsers":
22    "f0724bac-7
23  },
24  "includeGroups"
25  "excludeGroups"
26  "includeRoles":
27  "All"
28  "modifiedDateTime": "20
```

Entra ID Conditional Access View changes



The screenshot shows the Microsoft Azure portal interface for a user profile. The top navigation bar includes the Microsoft Azure logo and a search bar. The breadcrumb trail is Home > MSFT | Users > Users >. The user profile for Efi Bregman is displayed, with a search bar and action buttons (Edit properties, Delete, Refresh, Reset password). The left sidebar lists navigation options: Overview (selected), Audit logs, Sign-in logs, Diagnose and solve problems, Manage, and Troubleshooting + Support. The main content area shows the user's basic information, including a profile picture with initials 'EB', name 'Efi Bregman', email 'efibadmin@sstll.onmicrosoft.com', and role 'Member'. Below this is a table of user details.

User principal name	efibadmin@sstll.onmicrosoft.com
Object ID	f0724bac-72ab-4fef-a884-728a98b6d2b8
Created date time	May 21, 2024, 8:20 PM
User type	Member
Identities	sstll.onmicrosoft.com

CA Gatekeeper View changes

The screenshot displays the CA Gatekeeper interface with a blue header bar. On the left, there is a menu icon and the CA logo. On the right, there are icons for help, refresh, and a user profile. The main content area has a dark background and shows the following information:

Tenant: **Efi Demo Tenant**, Policy: **Require multifactor authentication for admins**, Protection Level: **None**

Timeline view (last 10) | Table view (all)

Timeline markers:

- 6/5/2024, 5:33:49 PM
- 6/5/2024, 6:21:07 PM
- Current configuration

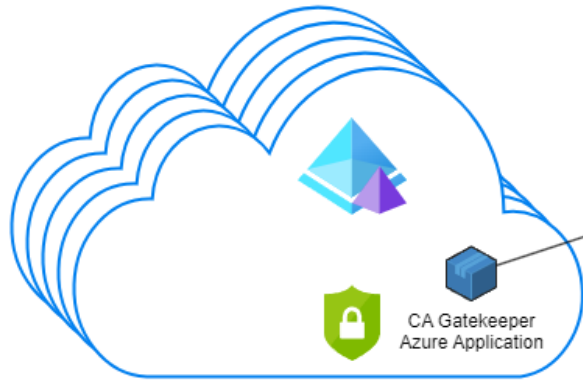
Policy: **Require multifactor authentication for admins**

What will happen if restored

- ▼ Collapse All
- ▼ conditions:
 - ▼ users:
 - ▼ excludeUsers:
 - + Efi Bregman

Restore

Architecture



Microsoft Entra ID (Tenant)

HTTPS
Microsoft Graph
<https://graph.microsoft.com>



Azure Customer Subscription

HTTPS
License Check
<https://cagkls.pro-vision.co.il>



Provision.io

CA Gatekeeper | API permissions

Search Refresh Got feedback?

- Overview
- Quickstart
- Integration assistant
- Manage
 - Branding & properties
 - Authentication
 - Certificates & secrets
 - Token configuration
 - API permissions**
 - Expose an API
 - App roles
 - Owners
 - Roles and administrators
 - Manifest
- Support + Troubleshooting

Configured permissions

Applications are authorized to call APIs when they are granted permissions by users/admins as part of the consent process. The list of configured permissions should include all the permissions the application needs. [Learn more about permissions and consent](#)

+ Add a permission Grant admin consent for Pro-Vision information Systems Ltd.

API / Permissions name	Type	Description	Admin consent required	Status
▼ Microsoft Graph (9)				
Agreement.Read.All	Application	Read all terms of use agreements	Yes	Granted
Application.Read.All	Application	Read all applications	Yes	Granted
AuditLog.Read.All	Application	Read all audit log data	Yes	Granted
CrossTenantInformation.ReadBasic.All	Application	Read cross-tenant basic information	Yes	Granted
Directory.Read.All	Application	Read directory data	Yes	Granted
Mail.Send	Application	Send mail as any user	Yes	Granted
Policy.Read.All	Application	Read your organization's policies	Yes	Granted
Policy.ReadWrite.ConditionalAccess	Application	Read and write your organization's conditional access policies	Yes	Granted
User.Read	Delegated	Sign in and read user profile	No	Granted

CA Gatekeeper

Demo



Thank You

<https://www.pro-vision.io/>

