
NIC
REBEL
EDITION

Importance of Zero Trust network access

Protection of People, Property and Assets

Secure access is critical for organizations to protect their people, property, and assets. Unauthorized access can lead to theft or reputational harm.

Importance of Access Control

Access control is important for organizations to ensure that only authorized personnel have access to restricted areas, data, or equipment, which can prevent theft, information leakage, and other security breaches.

NIC REBEL EDITION

POINT:TAKEN

Julian Rasmussen

A Journey into Entra ID Global Secure Access

https://www.linkedin.com/in/julianrasmussen

https://www.youtube.com/@Julianrasmussen

https://idefixwiki.no

@julianrasmussen.bsky.social

NIC REBEL EDITION

MVP Microsoft® Most Valuable Professional

Introduction

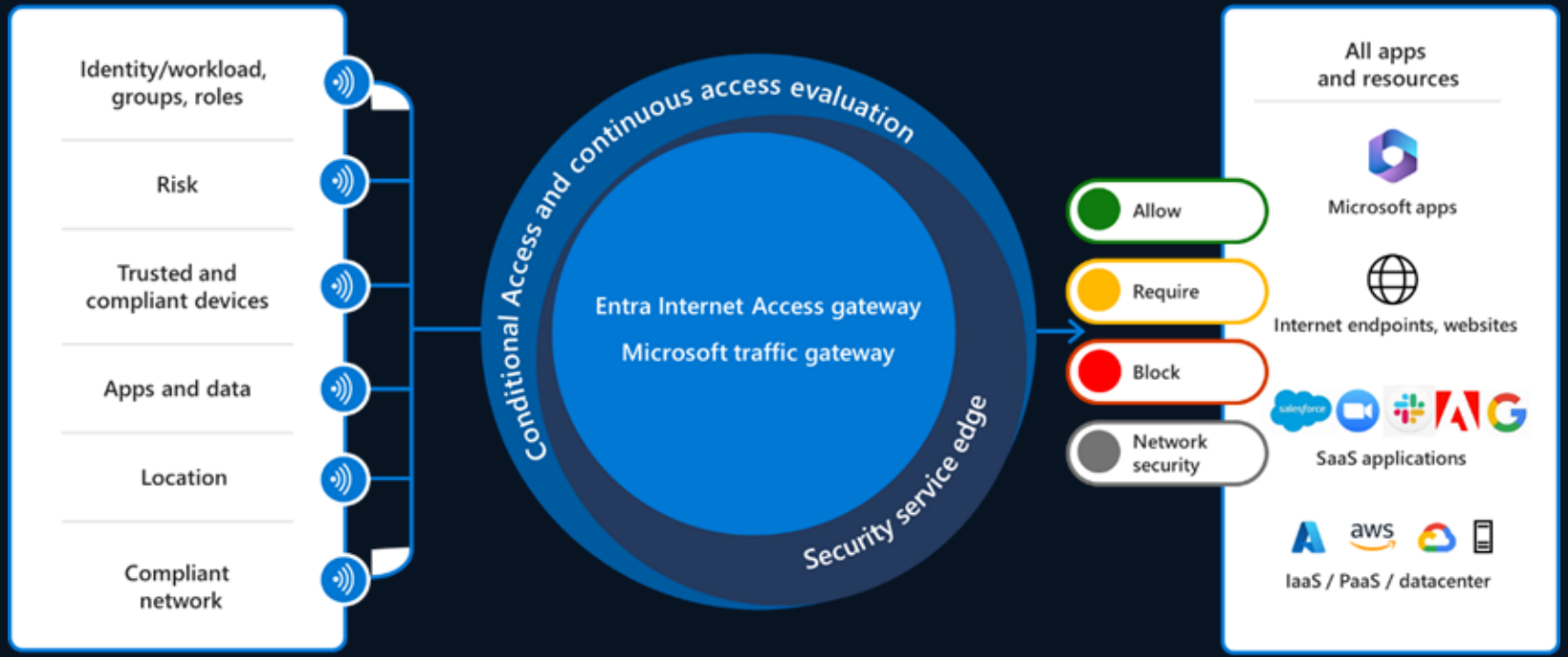
Entra ID Global Secure Access aims to provide innovative, reliable, and secure solutions that enable organizations to protect their people, property, and assets.

NIC REBEL EDITION

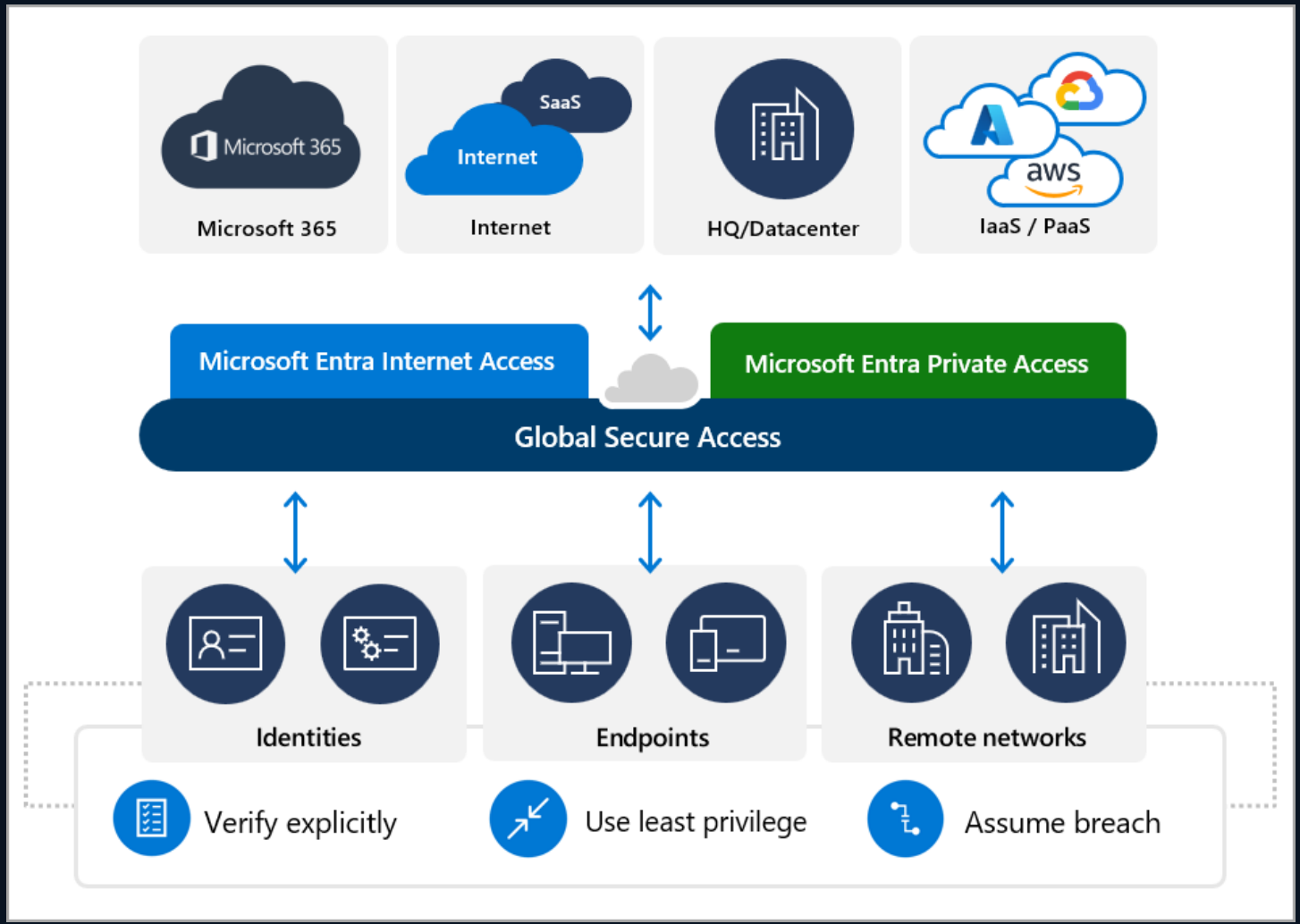
Signals

Evaluation

Execute



NIC REBEL EDITION

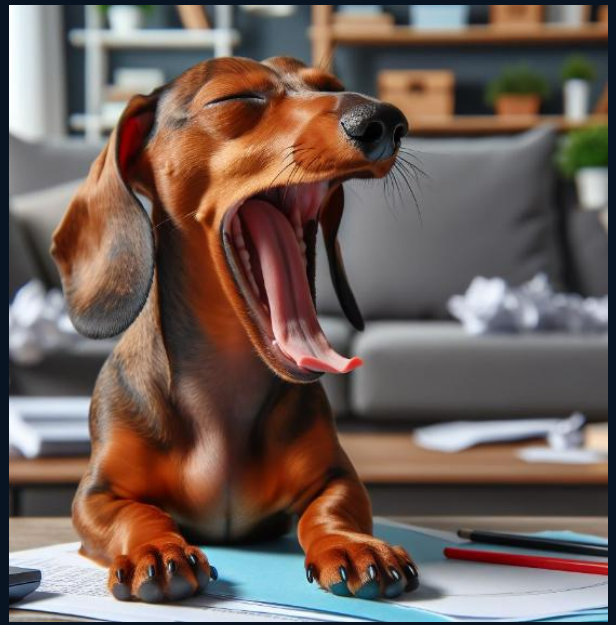


NIC REBEL EDITION

Licensing

Microsoft Entra Suite - $12/user/month

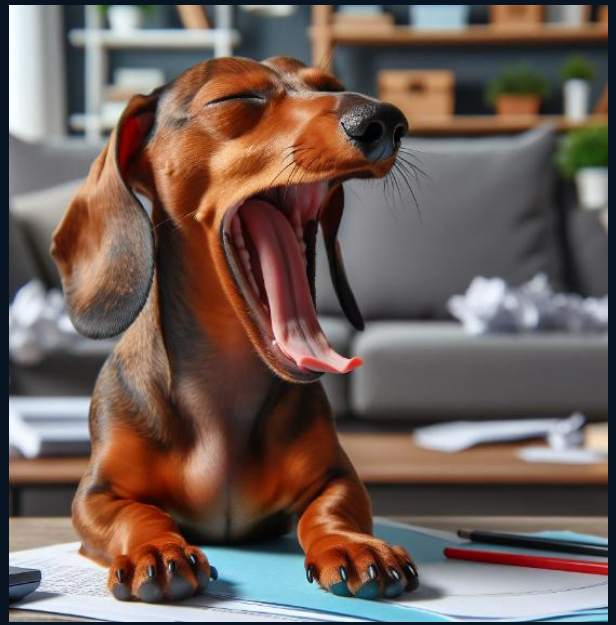
Add-on sku’s
Microsoft Entra Private Access - $5/user/month
Microsoft Entra Internet Access - $5/user/month



NIC REBEL EDITION

Licensing

Feature	Entra P1/P2 License - Microsoft traffic profile	Internet Access License* - Internet Access profile	Private Access License* - Private Access profile
Windows client	✅	✅	✅
macOS client	✅	✅	✅
Mobile client (iOS, Android)	✅	✅	✅
Traffic logs	✅	✅	✅
Remote network (branch connectivity)	✅	✅	
Universal Tenant Restrictions	✅		
Compliant network check	✅		
Source IP restoration	✅		
Microsoft 365 Enriched logs	✅		
Universal Conditional Access (CA)	✅	✅	
Context-aware network security		✅	
Web category filtering		✅	
Fully qualified domain name (FQDN) filtering		✅	
Universal Continuous Access Evaluation (CAE)	✅	✅	✅
VPN replacement with an identity-centric ZTNA			✅
Quick Access			✅
App Discovery			✅

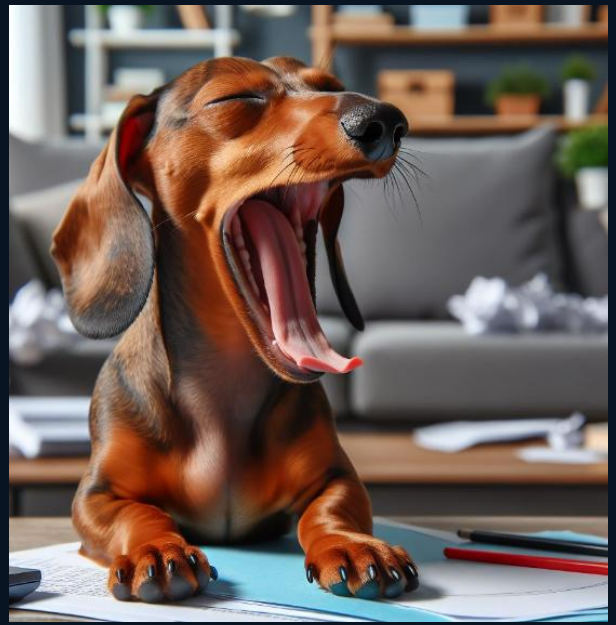


Feature	Entra P1/P2 License - Microsoft traffic profile	Internet Access License* - Internet Access profile	Private Access License* - Private Access profile
Windows client	✅	✅	✅
macOS client	✅	✅	✅
Mobile client (iOS, Android)	✅	✅	✅
Traffic logs	✅	✅	✅
Remote network (branch connectivity)	✅	✅	
Universal Tenant Restrictions	✅		
Compliant network check	✅		
Source IP restoration	✅		
Microsoft 365 Enriched logs	✅		
Universal Conditional Access (CA)	✅	✅	
Context-aware network security		✅	
Web category filtering		✅	

(CA)			
Context-aware network security		✓	
Web category filtering		✓	
Fully qualified domain name (FQDN) filtering		✓	
Universal Continuous Access Evaluation (CAE)	✓	✓	✓
VPN replacement with an identity-centric ZTNA			✓
Quick Access			✓
App Discovery			✓
Private Domain Name System (DNS)			✓
Single sign-on across all private apps			✓
Marketplace availability			✓
Private network connector multicloud support			✓

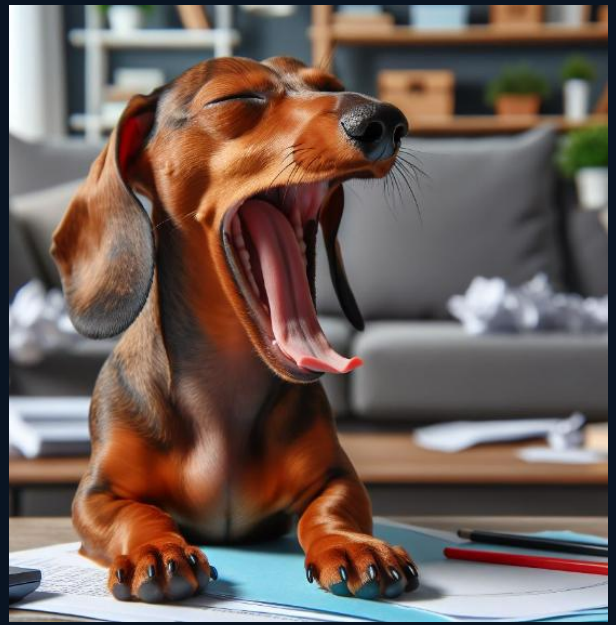
Licensing

Typical scenario
Microsoft 365 E3 + E5 Security + Entra Private Access
Microsoft 365 E3 + E5 Security + Entra Internet Access
Microsoft 365 E3 + E5 Security + Entra Suite



NIC REBEL EDITION

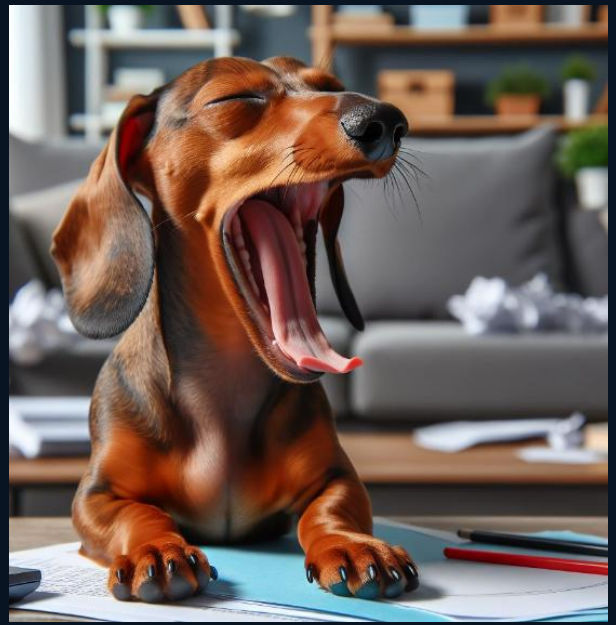
Microsoft Entra Internet Access for Microsoft services capabilities included in Entra ID P1/P2 License



NIC REBEL EDITION

Microsoft 365 Business Premium

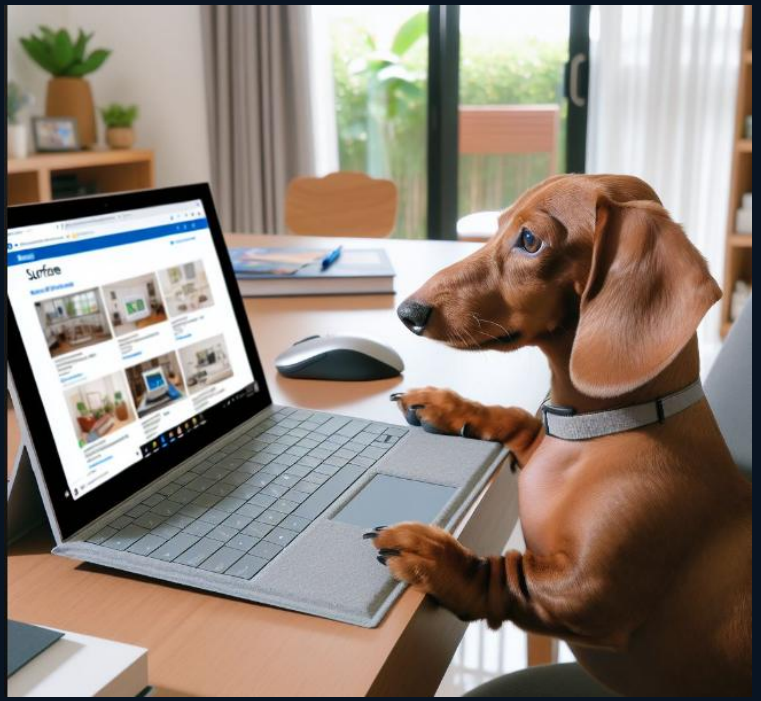
Internet Access for Microsoft Traffic



NIC REBEL EDITION

Microsoft Entra Internet Access

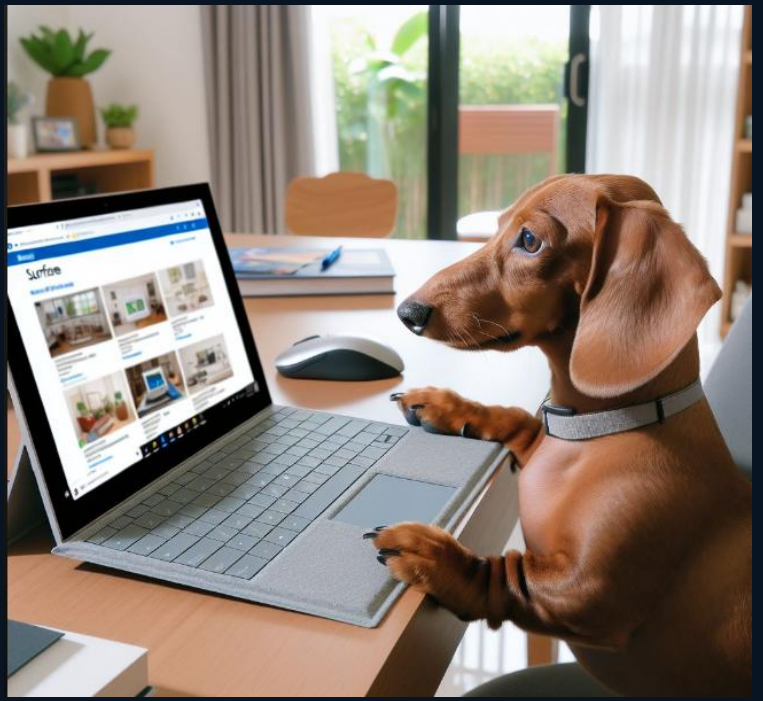
- Extend Conditional Access universally to all Internet endpoints
- Protect against data exfiltration
- Protect against token theft and prevent users from bypassing the secure network edge



NIC REBEL EDITION

Microsoft Entra Internet Access

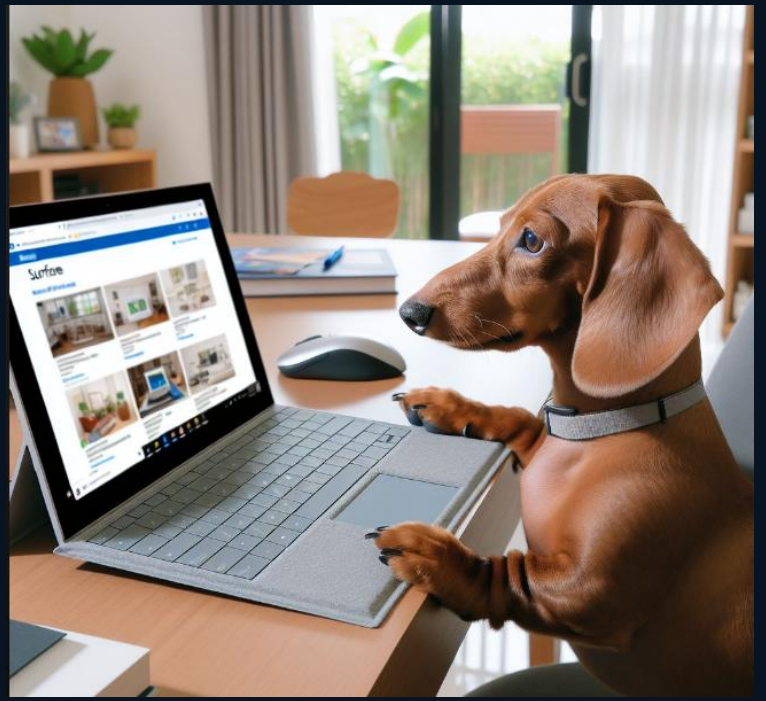
- Keeps original user source IP context for all traffic
- Unify network access controls with Conditional Access
- Restrict end user access to unsafe and non-compliant content



NIC REBEL EDITION

Microsoft Entra Internet Access

- Attain deep insights and network analytics using in-product dashboards
- Create custom views and dashboards based on rich insights into network logs
- Enriched real-time visibility for Microsoft 365 security events



NIC REBEL EDITION

Demo of setup for Microsoft Entra Internet Access

NIC REBEL EDITION

Home
Agents
Favorites
Entra ID
ID Governance
Verified ID
Permissions Management
Global Secure Access
What's new
Billing
Diagnose & solve problems
New support request

Microsoft Entra

Security Copilot agents are here

Discover a whole new way to automate security with AI.
Learn more about agents

Go to agents

Idefix

Tenant ID a16fc97f-b36a-48da-bf02-...
Primary domain idefix365.no

19 View users
49 View groups
10 View devices
19 View apps

Julian Fauskanger Rasmussen

Global Administrator

7cc05d64-a07b-46e7-9cac-5d1d3995b...
View user profile

My role assignments 3

High privileged role assignments
Other role assignments

Manage my roles

Users at high risk

No detections found

No user detections with risk level "high" in the last 365 days.

View high risk users

Shortcuts

Add | User sign-ins | Audit logs | Authentication Methods | Blocked users | Domain names | Unused service principals | Manage tenants | Named locations | Cross-tenant Access Policies | Tenant restrictions | Risk Based Conditional Access policies | Risky sign-ins | Lifecycle workflows

Get the most out of your licenses and subscriptions

Deployment guides

Use these deployment guides to plan, configure and deploy Microsoft Entra capabilities

Suggestions

- Modernize remote access to on-premises apps with MFA for each app
- Automate onboarding and manage user lifecycles with access to all applications
- Secure internet access based on specific business needs

Microsoft Entra plan

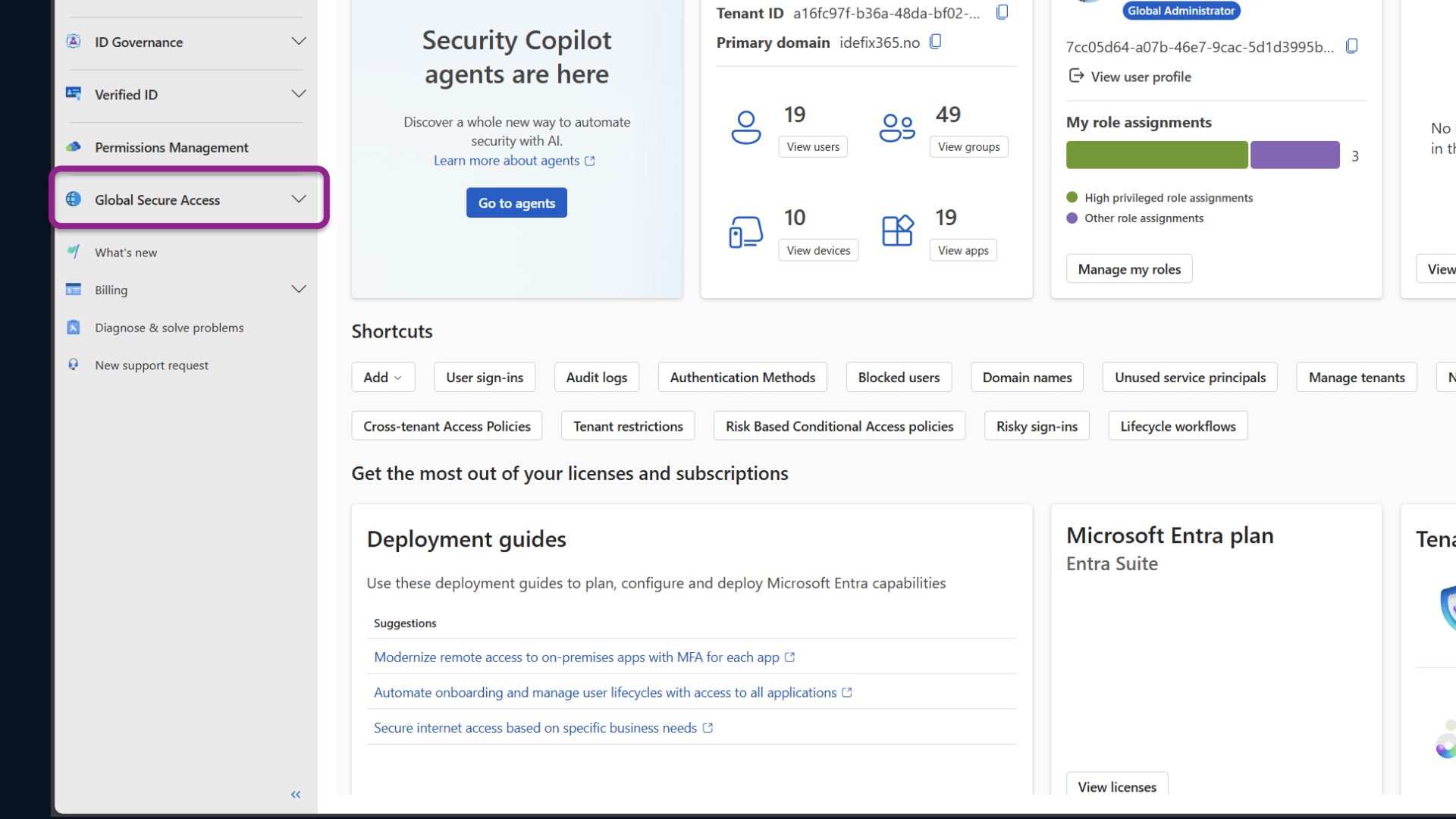
Entra Suite

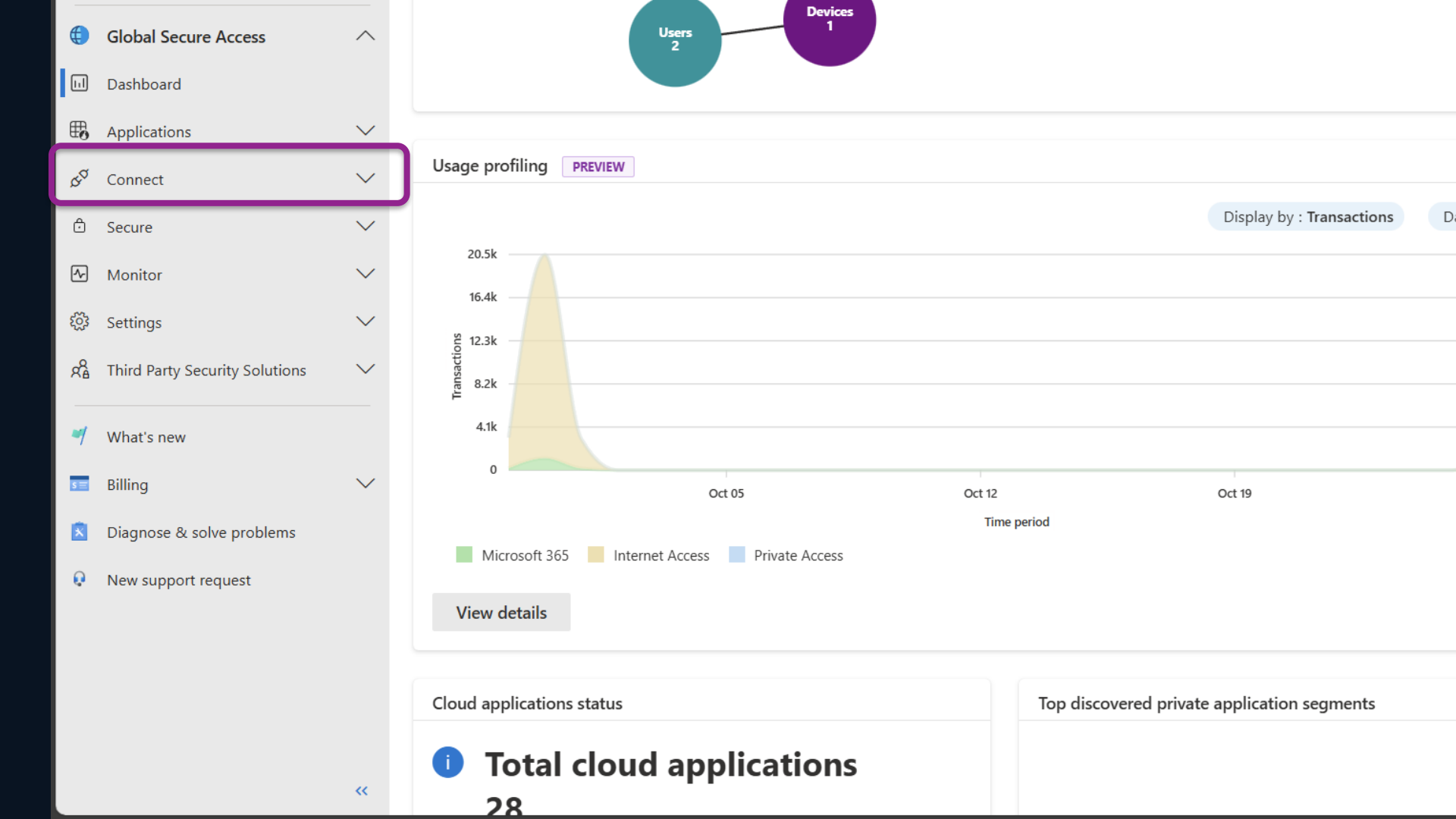
View licenses

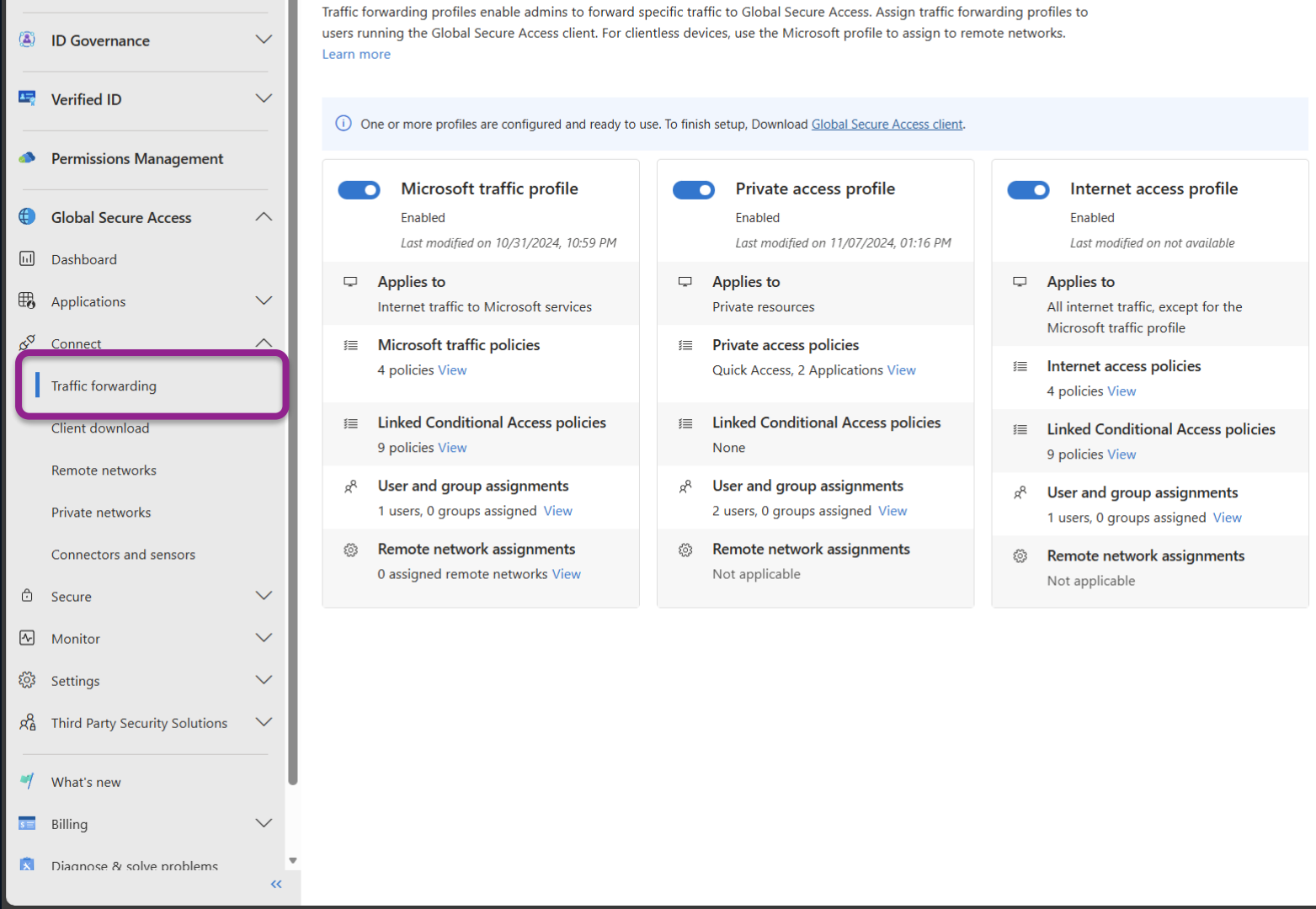
Tenant status

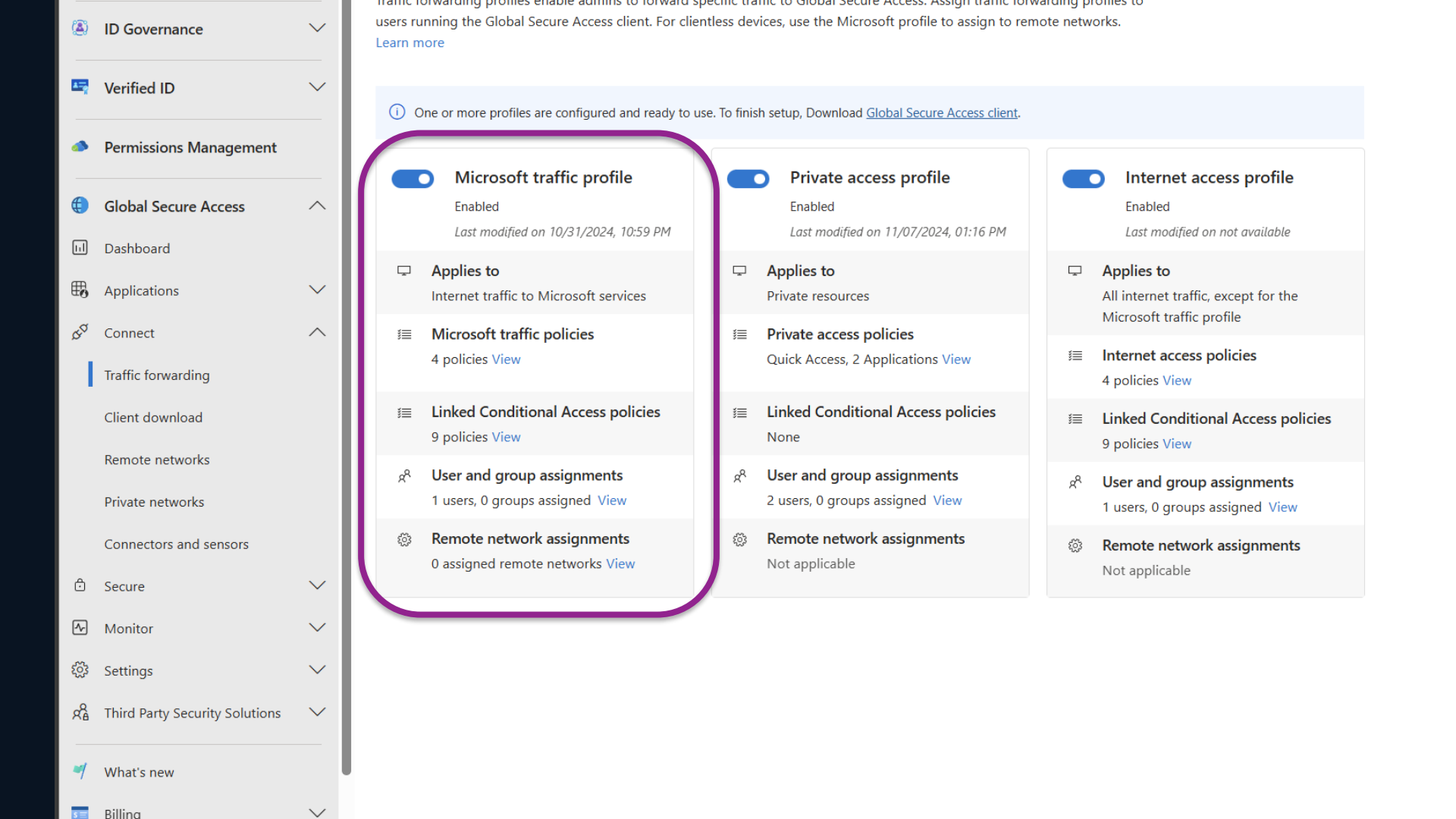
Identity Secure Score
55.84%
View recommendations

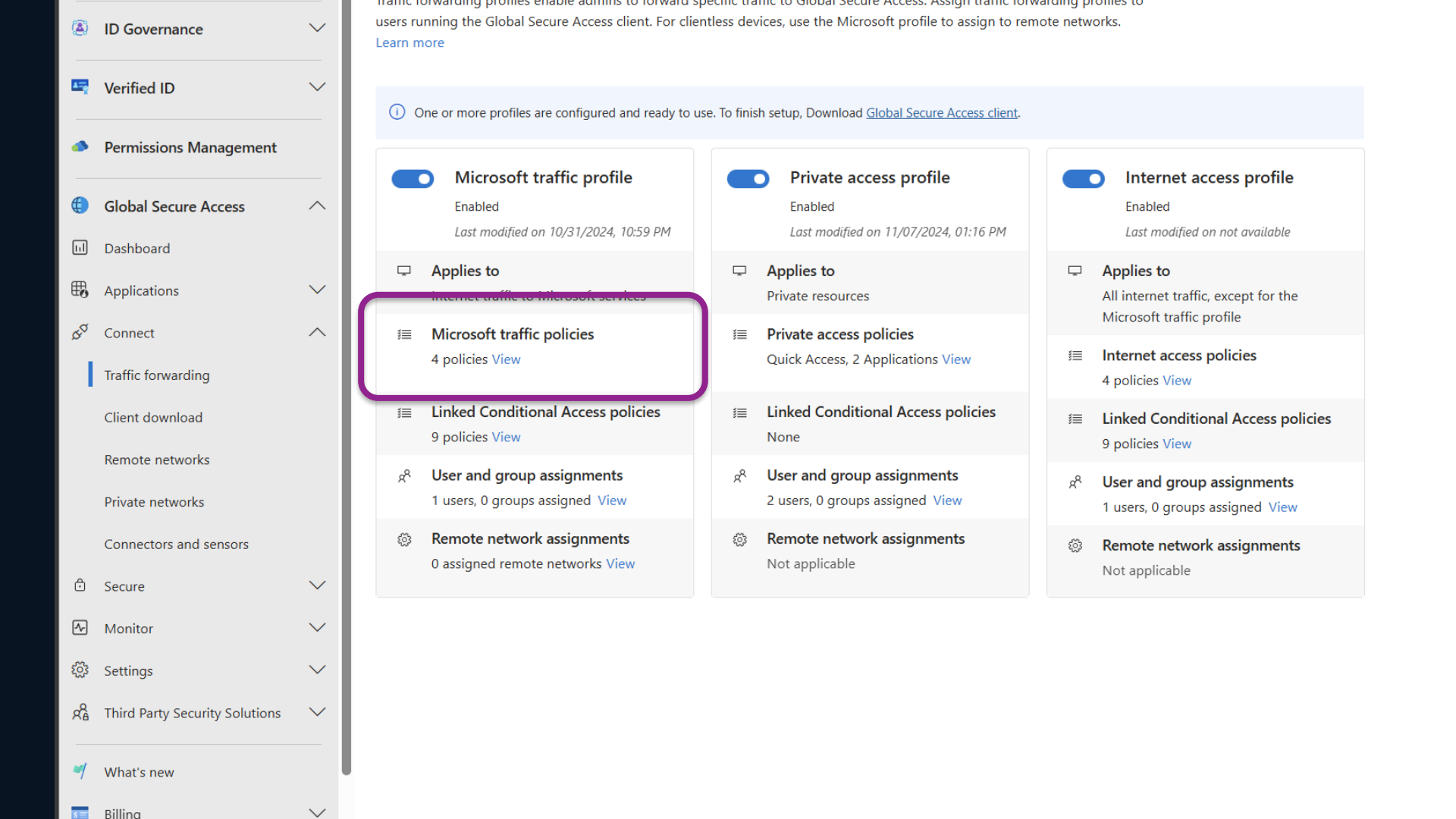
Microsoft Entra Connect
Disabled
View Entra Connect

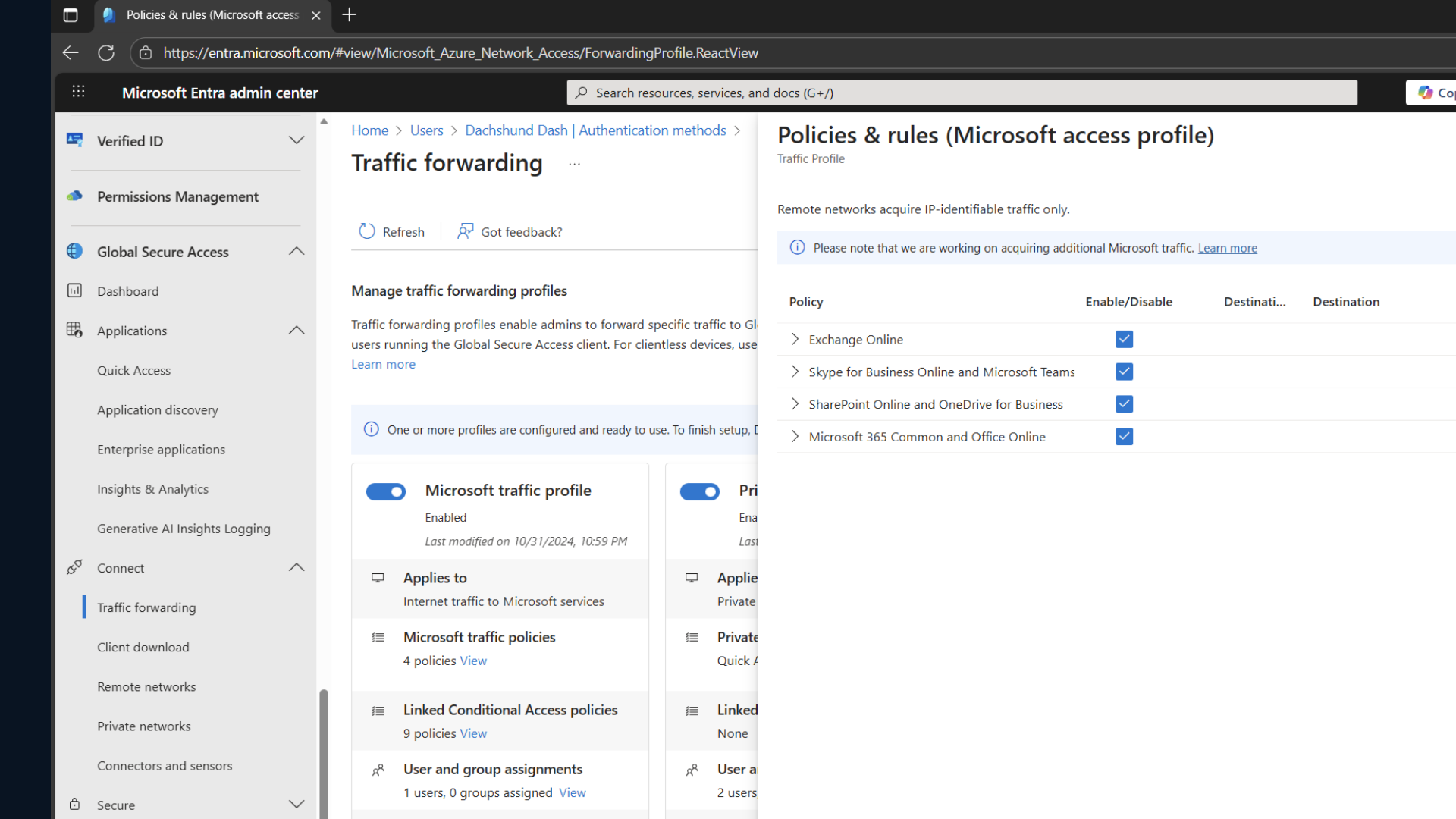

ID Governance
Verified ID
Permissions Management
Global Secure Access
What's new
Billing
Diagnose & solve problems
New support request
Security Copilot agents are here
Discover a whole new way to automate security with AI.
Learn more about agents
Go to agents
Tenant ID a16fc97f-b36a-48da-bf02-...
Primary domain idefix365.no
19
View users
49
View groups
10
View devices
19
View apps
Global Administrator
7cc05d64-a07b-46e7-9cac-5d1d3995b...
View user profile
My role assignments
3
High privileged role assignments
Other role assignments
Manage my roles
Shortcuts
Add
User sign-ins
Audit logs
Authentication Methods
Blocked users
Domain names
Unused service principals
Manage tenants
Cross-tenant Access Policies
Tenant restrictions
Risk Based Conditional Access policies
Risky sign-ins
Lifecycle workflows
Get the most out of your licenses and subscriptions
Deployment guides
Use these deployment guides to plan, configure and deploy Microsoft Entra capabilities
Suggestions
Modernize remote access to on-premises apps with MFA for each app
Automate onboarding and manage user lifecycles with access to all applications
Secure internet access based on specific business needs
Microsoft Entra plan
Entra Suite
View licenses

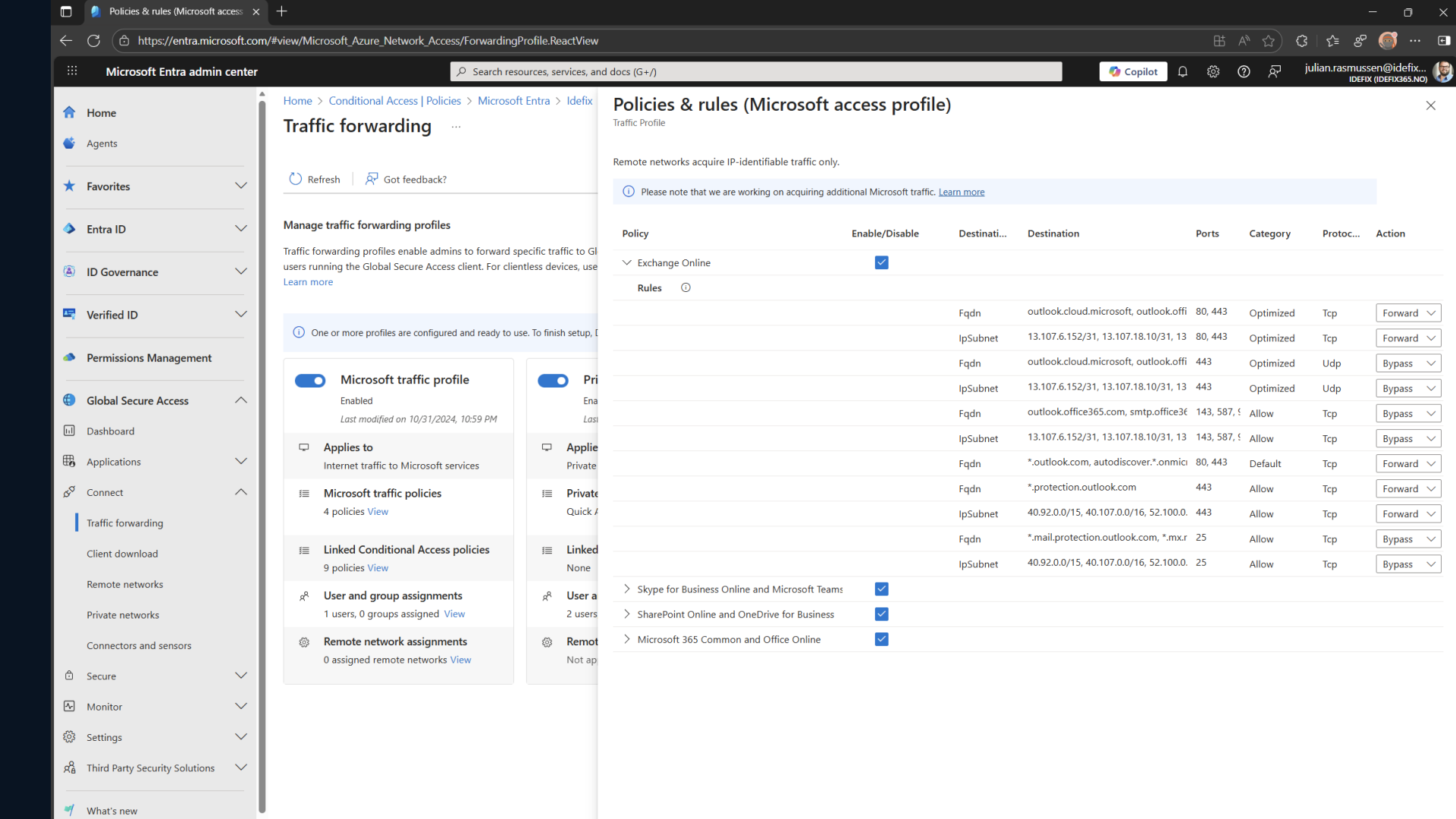

Global Secure Access
Dashboard
Applications
Connect
Secure
Monitor
Settings
Third Party Security Solutions
What's new
Billing
Diagnose & solve problems
New support request
Users 2
Devices 1
Usage profiling
PREVIEW
Display by : Transactions
20.5k
16.4k
12.3k
8.2k
4.1k
0
Transactions
Oct 05
Oct 12
Oct 19
Time period
Microsoft 365
Internet Access
Private Access
View details
Cloud applications status
Total cloud applications
28
Top discovered private application segments

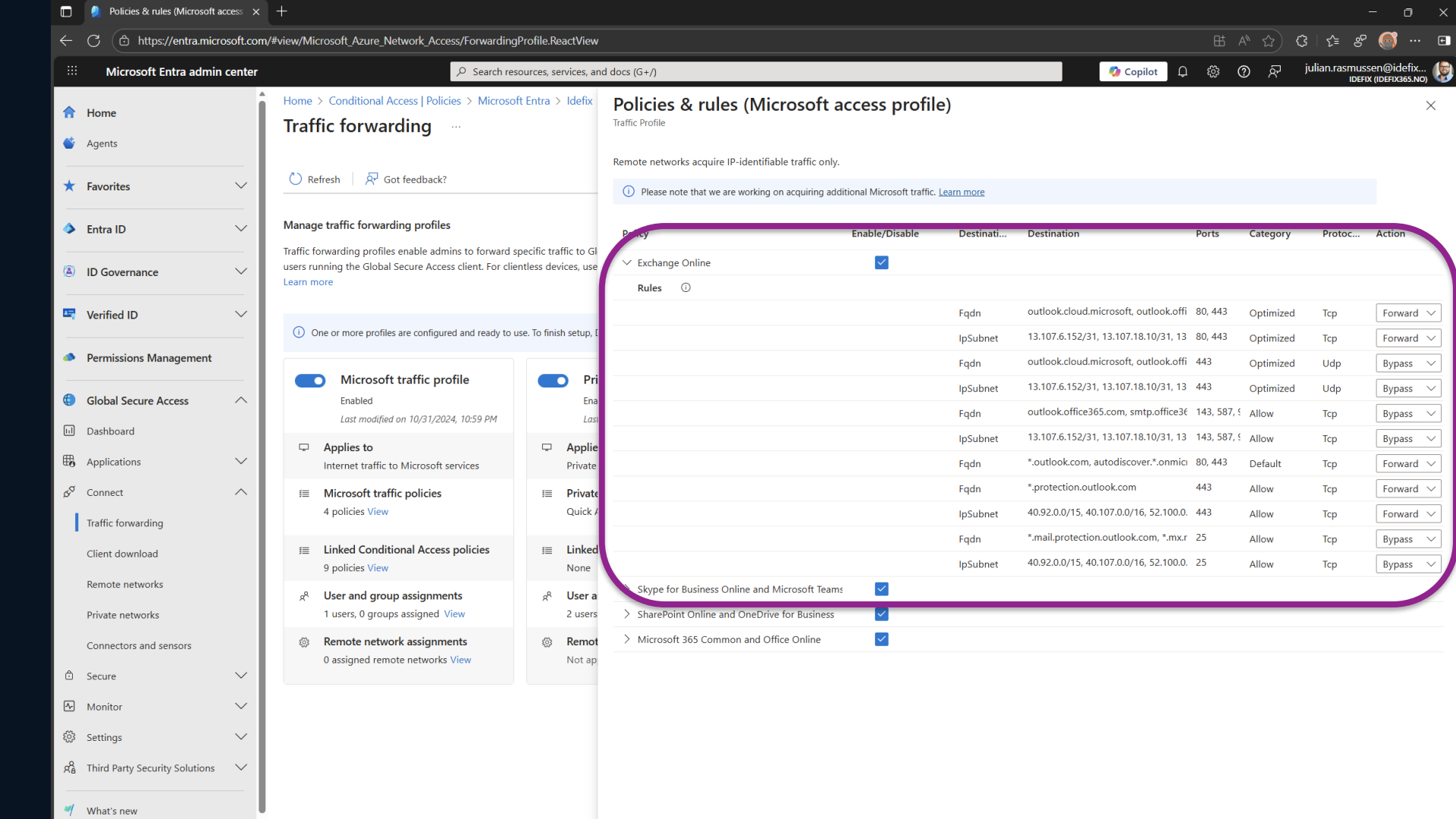

ID Governance
Verified ID
Permissions Management
Global Secure Access
Dashboard
Applications
Connect
Traffic forwarding
Client download
Remote networks
Private networks
Connectors and sensors
Secure
Monitor
Settings
Third Party Security Solutions
What's new
Billing
Diagnose & solve problems
Traffic forwarding profiles enable admins to forward specific traffic to Global Secure Access. Assign traffic forwarding profiles to users running the Global Secure Access client. For clientless devices, use the Microsoft profile to assign to remote networks.
Learn more
One or more profiles are configured and ready to use. To finish setup, Download Global Secure Access client.
Microsoft traffic profile
Enabled
Last modified on 10/31/2024, 10:59 PM
Applies to
Internet traffic to Microsoft services
Microsoft traffic policies
4 policies View
Linked Conditional Access policies
9 policies View
User and group assignments
1 users, 0 groups assigned View
Remote network assignments
0 assigned remote networks View
Private access profile
Enabled
Last modified on 11/07/2024, 01:16 PM
Applies to
Private resources
Private access policies
Quick Access, 2 Applications View
Linked Conditional Access policies
None
User and group assignments
2 users, 0 groups assigned View
Remote network assignments
Not applicable
Internet access profile
Enabled
Last modified on not available
Applies to
All internet traffic, except for the Microsoft traffic profile
Internet access policies
4 policies View
Linked Conditional Access policies
9 policies View
User and group assignments
1 users, 0 groups assigned View
Remote network assignments
Not applicable

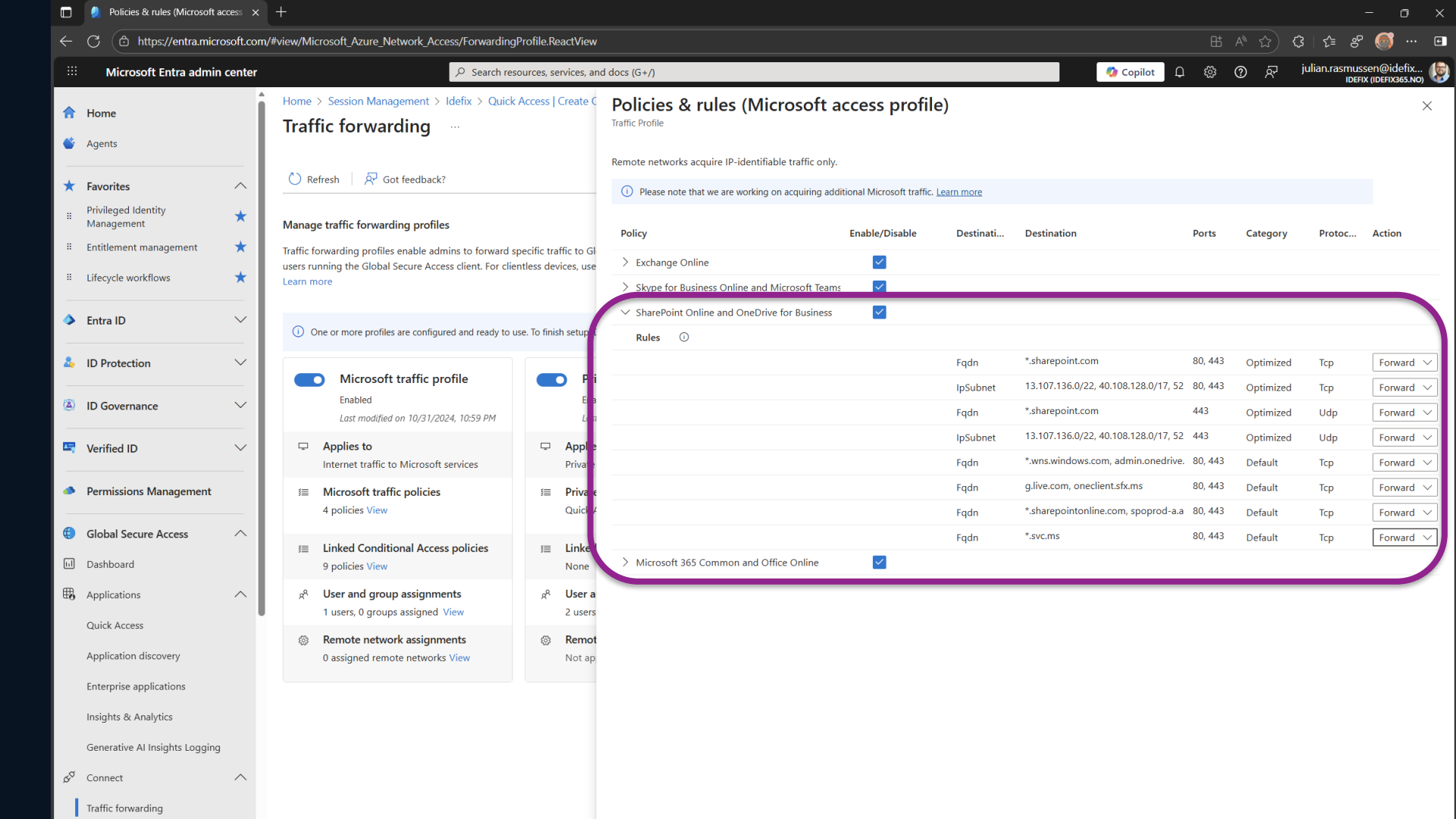

ID Governance
Verified ID
Permissions Management
Global Secure Access
Dashboard
Applications
Connect
Traffic forwarding
Client download
Remote networks
Private networks
Connectors and sensors
Secure
Monitor
Settings
Third Party Security Solutions
What's new
Billing
users running the Global Secure Access client. For clientless devices, use the Microsoft profile to assign to remote networks.
Learn more
One or more profiles are configured and ready to use. To finish setup, Download Global Secure Access client.
Microsoft traffic profile
Enabled
Last modified on 10/31/2024, 10:59 PM
Applies to
Internet traffic to Microsoft services
Microsoft traffic policies
4 policies View
Linked Conditional Access policies
9 policies View
User and group assignments
1 users, 0 groups assigned View
Remote network assignments
0 assigned remote networks View
Private access profile
Enabled
Last modified on 11/07/2024, 01:16 PM
Applies to
Private resources
Private access policies
Quick Access, 2 Applications View
Linked Conditional Access policies
None
User and group assignments
2 users, 0 groups assigned View
Remote network assignments
Not applicable
Internet access profile
Enabled
Last modified on not available
Applies to
All internet traffic, except for the Microsoft traffic profile
Internet access policies
4 policies View
Linked Conditional Access policies
9 policies View
User and group assignments
1 users, 0 groups assigned View
Remote network assignments
Not applicable


ID Governance
Verified ID
Permissions Management
Global Secure Access
Dashboard
Applications
Connect
Traffic forwarding
Client download
Remote networks
Private networks
Connectors and sensors
Secure
Monitor
Settings
Third Party Security Solutions
What's new
Billing
users running the Global Secure Access client. For clientless devices, use the Microsoft profile to assign to remote networks.
Learn more
One or more profiles are configured and ready to use. To finish setup, Download Global Secure Access client.
Microsoft traffic profile
Enabled
Last modified on 10/31/2024, 10:59 PM
Applies to
Microsoft traffic policies
4 policies View
Linked Conditional Access policies
9 policies View
User and group assignments
1 users, 0 groups assigned View
Remote network assignments
0 assigned remote networks View
Private access profile
Enabled
Last modified on 11/07/2024, 01:16 PM
Applies to
Private resources
Private access policies
Quick Access, 2 Applications View
Linked Conditional Access policies
None
User and group assignments
2 users, 0 groups assigned View
Remote network assignments
Not applicable
Internet access profile
Enabled
Last modified on not available
Applies to
All internet traffic, except for the Microsoft traffic profile
Internet access policies
4 policies View
Linked Conditional Access policies
9 policies View
User and group assignments
1 users, 0 groups assigned View
Remote network assignments
Not applicable


Policies & rules (Microsoft access
https://entra.microsoft.com/#view/Microsoft_Azure_Network_Access/ForwardingProfile.ReactView
Microsoft Entra admin center
Search resources, services, and docs (G+/)
Verified ID
Permissions Management
Global Secure Access
Dashboard
Applications
Quick Access
Application discovery
Enterprise applications
Insights & Analytics
Generative AI Insights Logging
Connect
Traffic forwarding
Client download
Remote networks
Private networks
Connectors and sensors
Secure
Home > Users > Dachshund Dash | Authentication methods >
Traffic forwarding
Refresh
Got feedback?
Manage traffic forwarding profiles
Traffic forwarding profiles enable admins to forward specific traffic to Gl
users running the Global Secure Access client. For clientless devices, use
Learn more
One or more profiles are configured and ready to use. To finish setup, D
Microsoft traffic profile
Enabled
Last modified on 10/31/2024, 10:59 PM
Applies to
Internet traffic to Microsoft services
Microsoft traffic policies
4 policies View
Linked Conditional Access policies
9 policies View
User and group assignments
1 users, 0 groups assigned View
Policies & rules (Microsoft access profile)
Traffic Profile
Remote networks acquire IP-identifiable traffic only.
Please note that we are working on acquiring additional Microsoft traffic. Learn more
Policy
Enable/Disable
Destinati...
Destination
Exchange Online
Skype for Business Online and Microsoft Teams
SharePoint Online and OneDrive for Business
Microsoft 365 Common and Office Online


Policies & rules (Microsoft access
https://entra.microsoft.com/#view/Microsoft_Azure_Network_Access/ForwardingProfile.ReactView
Microsoft Entra admin center
Search resources, services, and docs (G+/)
Copilot
julian.rasmussen@idefix...
IDEFIX (IDEFIX365.NO)
Home
Agents
Favorites
Entra ID
ID Governance
Verified ID
Permissions Management
Global Secure Access
Dashboard
Applications
Connect
Traffic forwarding
Client download
Remote networks
Private networks
Connectors and sensors
Secure
Monitor
Settings
Third Party Security Solutions
What's new
Home > Conditional Access | Policies > Microsoft Entra > Idefix
Traffic forwarding
Refresh
Got feedback?
Manage traffic forwarding profiles
Traffic forwarding profiles enable admins to forward specific traffic to Gl
users running the Global Secure Access client. For clientless devices, use
Learn more
One or more profiles are configured and ready to use. To finish setup,
Microsoft traffic profile
Enabled
Last modified on 10/31/2024, 10:59 PM
Applies to
Internet traffic to Microsoft services
Microsoft traffic policies
4 policies View
Linked Conditional Access policies
9 policies View
User and group assignments
1 users, 0 groups assigned View
Remote network assignments
0 assigned remote networks View
Policies & rules (Microsoft access profile)
Traffic Profile
Remote networks acquire IP-identifiable traffic only.
Please note that we are working on acquiring additional Microsoft traffic. Learn more
Policy
Enable/Disable
Destinati...
Destination
Ports
Category
Protoc...
Action
Exchange Online
Rules
Fqdn outlook.cloud.microsoft, outlook.offi 80, 443 Optimized Tcp Forward
IpSubnet 13.107.6.152/31, 13.107.18.10/31, 13 80, 443 Optimized Tcp Forward
Fqdn outlook.cloud.microsoft, outlook.offi 443 Optimized Udp Bypass
IpSubnet 13.107.6.152/31, 13.107.18.10/31, 13 443 Optimized Udp Bypass
Fqdn outlook.office365.com, smtp.office36 143, 587, Allow Tcp Bypass
IpSubnet 13.107.6.152/31, 13.107.18.10/31, 13 143, 587, Allow Tcp Bypass
Fqdn *.outlook.com, autodiscover.*.onmicr 80, 443 Default Tcp Forward
Fqdn *.protection.outlook.com 443 Allow Tcp Forward
IpSubnet 40.92.0.0/15, 40.107.0.0/16, 52.100.0. 443 Allow Tcp Forward
Fqdn *.mail.protection.outlook.com, *.mx.r 25 Allow Tcp Bypass
IpSubnet 40.92.0.0/15, 40.107.0.0/16, 52.100.0. 25 Allow Tcp Bypass
Skype for Business Online and Microsoft Teams
SharePoint Online and OneDrive for Business
Microsoft 365 Common and Office Online


Policies & rules (Microsoft access
https://entra.microsoft.com/#view/Microsoft_Azure_Network_Access/ForwardingProfile.ReactView
Microsoft Entra admin center
Search resources, services, and docs (G+/)
Copilot
julian.rasmussen@idefix...
IDEFIX (IDEFIX365.NO)
Home
Agents
Favorites
Entra ID
ID Governance
Verified ID
Permissions Management
Global Secure Access
Dashboard
Applications
Connect
Traffic forwarding
Client download
Remote networks
Private networks
Connectors and sensors
Secure
Monitor
Settings
Third Party Security Solutions
What's new
Home > Conditional Access | Policies > Microsoft Entra > Idefix
Traffic forwarding
Refresh
Got feedback?
Manage traffic forwarding profiles
Traffic forwarding profiles enable admins to forward specific traffic to Gl
users running the Global Secure Access client. For clientless devices, use
Learn more
One or more profiles are configured and ready to use. To finish setup,
Microsoft traffic profile
Enabled
Last modified on 10/31/2024, 10:59 PM
Applies to
Internet traffic to Microsoft services
Microsoft traffic policies
4 policies View
Linked Conditional Access policies
9 policies View
User and group assignments
1 users, 0 groups assigned View
Remote network assignments
0 assigned remote networks View
Policies & rules (Microsoft access profile)
Traffic Profile
Remote networks acquire IP-identifiable traffic only.
Please note that we are working on acquiring additional Microsoft traffic. Learn more
Policy
Enable/Disable
Destinati...
Destination
Ports
Category
Protoc...
Action
Exchange Online
Rules
Fqdn outlook.cloud.microsoft, outlook.offi 80, 443 Optimized Tcp Forward
IpSubnet 13.107.6.152/31, 13.107.18.10/31, 13 80, 443 Optimized Tcp Forward
Fqdn outlook.cloud.microsoft, outlook.offi 443 Optimized Udp Bypass
IpSubnet 13.107.6.152/31, 13.107.18.10/31, 13 443 Optimized Udp Bypass
Fqdn outlook.office365.com, smtp.office3 143, 587, Allow Tcp Bypass
IpSubnet 13.107.6.152/31, 13.107.18.10/31, 13 143, 587, Allow Tcp Bypass
Fqdn *.outlook.com, autodiscover.*.onmic 80, 443 Default Tcp Forward
Fqdn *.protection.outlook.com 443 Allow Tcp Forward
IpSubnet 40.92.0.0/15, 40.107.0.0/16, 52.100.0. 443 Allow Tcp Forward
Fqdn *.mail.protection.outlook.com, *.mx.r 25 Allow Tcp Bypass
IpSubnet 40.92.0.0/15, 40.107.0.0/16, 52.100.0. 25 Allow Tcp Bypass
Skype for Business Online and Microsoft Teams
SharePoint Online and OneDrive for Business
Microsoft 365 Common and Office Online


Policies & rules (Microsoft access
https://entra.microsoft.com/#view/Microsoft_Azure_Network_Access/ForwardingProfile.ReactView
Microsoft Entra admin center
Search resources, services, and docs (G+/)
Copilot
julian.rasmussen@idefix...
IDEFIX (IDEFIX365.NO)
Home
Agents
Favorites
Privileged Identity Management
Entitlement management
Lifecycle workflows
Entra ID
ID Protection
ID Governance
Verified ID
Permissions Management
Global Secure Access
Dashboard
Applications
Quick Access
Application discovery
Enterprise applications
Insights & Analytics
Generative AI Insights Logging
Connect
Traffic forwarding
Home > Session Management > Idefix > Quick Access | Create C
Traffic forwarding
Refresh
Got feedback?
Manage traffic forwarding profiles
Traffic forwarding profiles enable admins to forward specific traffic to Gl
users running the Global Secure Access client. For clientless devices, use
Learn more
One or more profiles are configured and ready to use. To finish setup
Microsoft traffic profile
Enabled
Last modified on 10/31/2024, 10:59 PM
Applies to
Internet traffic to Microsoft services
Microsoft traffic policies
4 policies View
Linked Conditional Access policies
9 policies View
User and group assignments
1 users, 0 groups assigned View
Remote network assignments
0 assigned remote networks View
Policies & rules (Microsoft access profile)
Traffic Profile
Remote networks acquire IP-identifiable traffic only.
Please note that we are working on acquiring additional Microsoft traffic. Learn more
Policy
Enable/Disable
Destinati...
Destination
Ports
Category
Protoc...
Action
Exchange Online
Skype for Business Online and Microsoft Teams
SharePoint Online and OneDrive for Business
Rules
Fqdn *.sharepoint.com 80, 443 Optimized Tcp Forward
IpSubnet 13.107.136.0/22, 40.108.128.0/17, 52 80, 443 Optimized Tcp Forward
Fqdn *.sharepoint.com 443 Optimized Udp Forward
IpSubnet 13.107.136.0/22, 40.108.128.0/17, 52 443 Optimized Udp Forward
Fqdn *.wns.windows.com, admin.onedrive. 80, 443 Default Tcp Forward
Fqdn g.live.com, oneclient.sfx.ms 80, 443 Default Tcp Forward
Fqdn *.sharepointonline.com, spoprod-a.a 80, 443 Default Tcp Forward
Fqdn *.svc.ms 80, 443 Default Tcp Forward
Microsoft 365 Common and Office Online

Manage traffic forwarding profiles

Traffic forwarding profiles enable admins to forward specific traffic to Global Secure Access. Assign traffic forwarding profiles to users running the Global Secure Access client. For clientless devices, use the Microsoft profile to assign to remote networks.
Learn more

One or more profiles are configured and ready to use. To finish setup, Download Global Secure Access client.

Microsoft traffic profile

Enabled

Last modified on 10/31/2024, 10:59 PM

Applies to
Internet traffic to Microsoft services

Microsoft traffic policies
3 policies View

Linked Conditional Access policies
2 policies View

User and group assignments
1 users, 0 groups assigned View

Remote network assignments
0 assigned remote networks View

Private access profile

Enabled

Last modified on 10/29/2024, 09:36 PM

Applies to
Private resources

Private access policies
Quick Access, 0 Applications

Linked Conditional Access policies
None

User and group assignments
2 users, 0 groups assigned View

Remote network assignments
Not applicable

Internet access profile

Enabled

Last modified on not available

Applies to
All internet traffic, except for the Microsoft traffic profile

Internet access policies
3 policies View

Linked Conditional Access policies
2 policies View

User and group assignments
2 users, 0 groups assigned View

Remote network assignments
Not applicable

Home
What's new
Diagnose & solve problems
Favorites
Privileged Identity Management
All users
Identity
Protection
Identity Governance
Verified ID
Permissions Management
Global Secure Access
Dashboard
Applications
Connect
Traffic forwarding
Client download
Remote networks
Connectors
Secure
Monitor
Learn & support

Traffic forwarding

Global Secure Access is now in generally available. Licensing requirements have been updated. Licensing enforcement for Microsoft Entra Private Access, Microsoft Entra Inte with General Availability on July 1st, 2024. Learn more

Refresh | Got feedback?

Manage traffic forwarding profiles

Traffic forwarding profiles enable admins to forward specific traffic to Global Secure Access. Assign traffic forwarding profiles to users running the Global Secure Access client. For clientless devices, use the Microsoft profile to assign to remote networks.
Learn more

One or more profiles are configured and ready to use. To finish setup, Download Global Secure Access client.

Microsoft traffic profile

Enabled
Last modified on 10/31/2024, 10:59 PM

Applies to
Internet traffic to Microsoft services

Microsoft traffic policies
3 policies View

Linked Conditional Access policies
2 policies View

User and group assignments
1 users, 0 groups assigned View

Remote network assignments
0 assigned remote networks View

Private access profile

Enabled
Last modified on 10/29/2024, 09:36 PM

Applies to
Private resources

Private access policies
Quick Access, 0 Applications

Linked Conditional Access policies
None

User and group assignments
2 users, 0 groups assigned View

Remote network assignments
Not applicable

Internet access profile

Enabled
Last modified on not available

Applies to
All internet traffic, except for the Microsoft traffic profile

Internet access policies
3 policies View

Linked Conditional Access policies
2 policies View

User and group assignments
2 users, 0 groups assigned View

Remote network assignments
Not applicable

User and group assignments

Microsoft profile

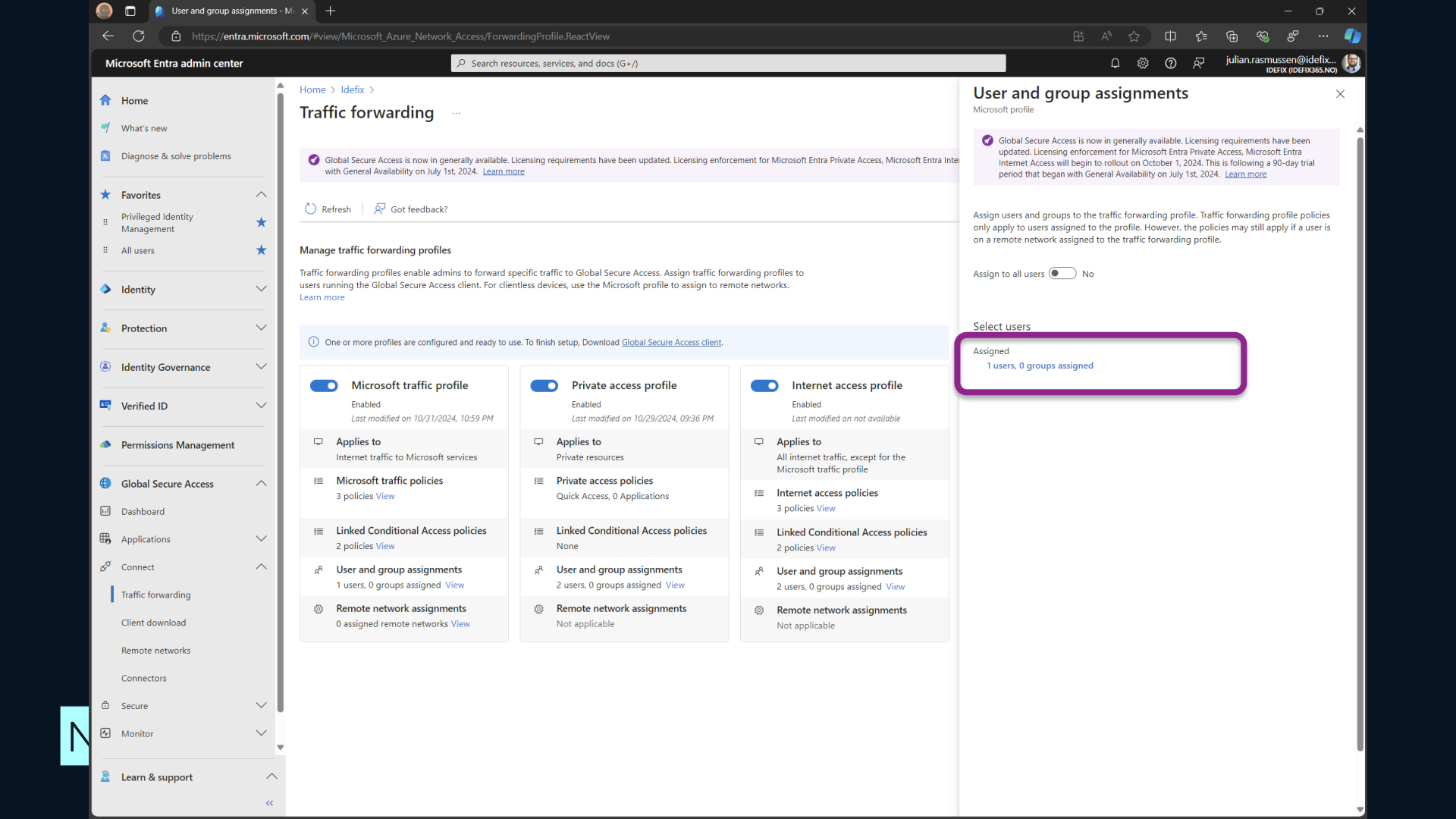
Global Secure Access is now in generally available. Licensing requirements have been updated. Licensing enforcement for Microsoft Entra Private Access, Microsoft Entra Internet Access will begin to rollout on October 1, 2024. This is following a 90-day trial period that began with General Availability on July 1st, 2024. Learn more

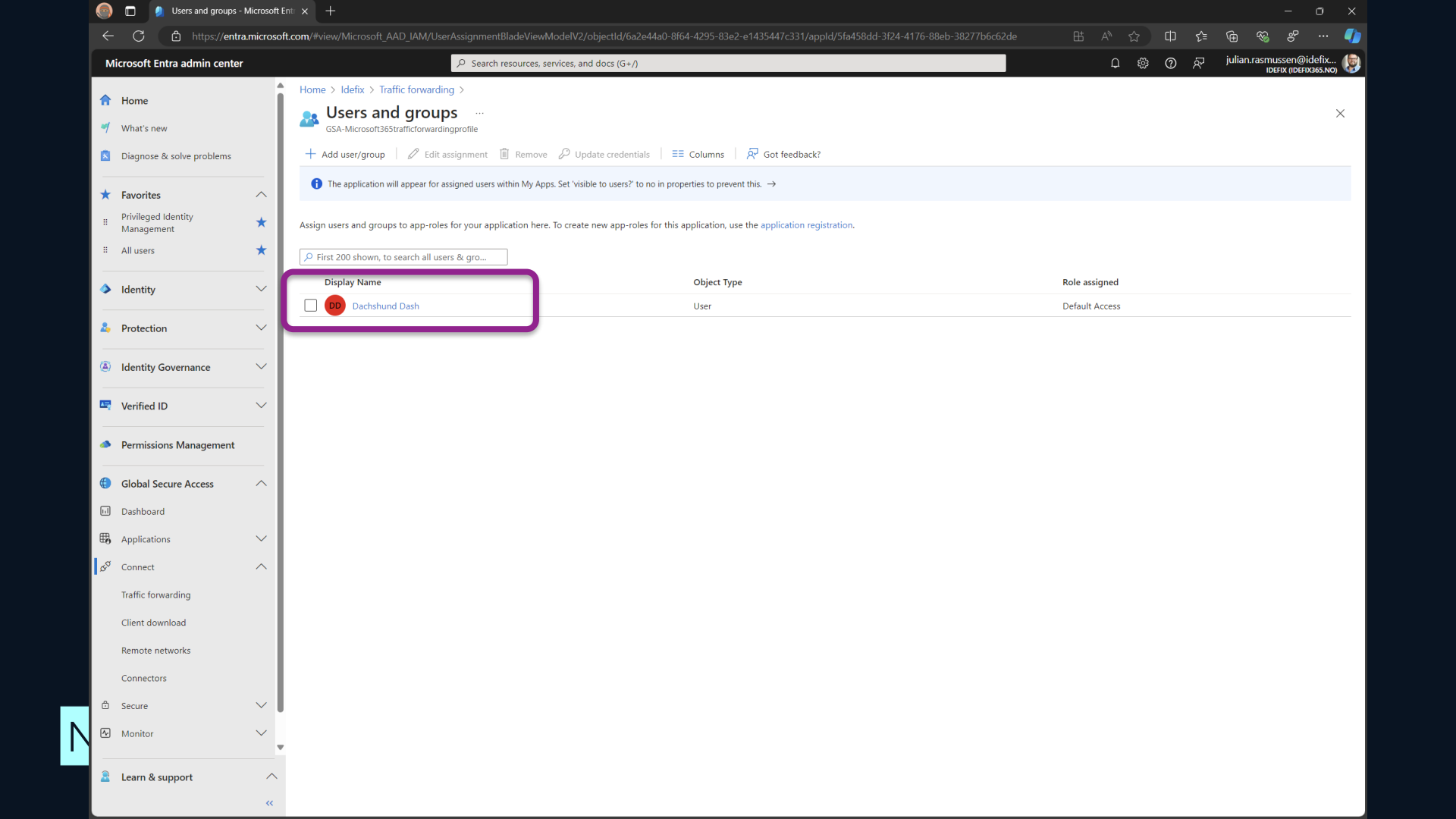
Assign users and groups to the traffic forwarding profile. Traffic forwarding profile policies only apply to users assigned to the profile. However, the policies may still apply if a user is on a remote network assigned to the traffic forwarding profile.

Assign to all users No

Select users

Assigned
1 users, 0 groups assigned


User and group assignments - Mi
https://entra.microsoft.com/#view/Microsoft_Azure_Network_Access/ForwardingProfile.ReactView
Microsoft Entra admin center
Search resources, services, and docs (G+/)
julian.rasmussen@idefix...
IDEFIX (IDEFIX365.NO)
Home
What's new
Diagnose & solve problems
Favorites
Privileged Identity Management
All users
Identity
Protection
Identity Governance
Verified ID
Permissions Management
Global Secure Access
Dashboard
Applications
Connect
Traffic forwarding
Client download
Remote networks
Connectors
Secure
Monitor
Learn & support
Home > Idefix >
Traffic forwarding
Global Secure Access is now in generally available. Licensing requirements have been updated. Licensing enforcement for Microsoft Entra Private Access, Microsoft Entra Inte
with General Availability on July 1st, 2024. Learn more
Refresh
Got feedback?
Manage traffic forwarding profiles
Traffic forwarding profiles enable admins to forward specific traffic to Global Secure Access. Assign traffic forwarding profiles to users running the Global Secure Access client. For clientless devices, use the Microsoft profile to assign to remote networks.
Learn more
One or more profiles are configured and ready to use. To finish setup, Download Global Secure Access client.
Microsoft traffic profile
Enabled
Last modified on 10/31/2024, 10:59 PM
Applies to
Internet traffic to Microsoft services
Microsoft traffic policies
3 policies View
Linked Conditional Access policies
2 policies View
User and group assignments
1 users, 0 groups assigned View
Remote network assignments
0 assigned remote networks View
Private access profile
Enabled
Last modified on 10/29/2024, 09:36 PM
Applies to
Private resources
Private access policies
Quick Access, 0 Applications
Linked Conditional Access policies
None
User and group assignments
2 users, 0 groups assigned View
Remote network assignments
Not applicable
Internet access profile
Enabled
Last modified on not available
Applies to
All internet traffic, except for the Microsoft traffic profile
Internet access policies
3 policies View
Linked Conditional Access policies
2 policies View
User and group assignments
2 users, 0 groups assigned View
Remote network assignments
Not applicable
User and group assignments
Microsoft profile
Global Secure Access is now in generally available. Licensing requirements have been updated. Licensing enforcement for Microsoft Entra Private Access, Microsoft Entra Internet Access will begin to rollout on October 1, 2024. This is following a 90-day trial period that began with General Availability on July 1st, 2024. Learn more
Assign users and groups to the traffic forwarding profile. Traffic forwarding profile policies only apply to users assigned to the profile. However, the policies may still apply if a user is on a remote network assigned to the traffic forwarding profile.
Assign to all users
No
Select users
Assigned
1 users, 0 groups assigned


Users and groups - Microsoft Entra admin center
https://entra.microsoft.com/#view/Microsoft_AAD_IAM/UserAssignmentBladeViewModelV2/objectId/6a2e44a0-8f64-4295-83e2-e1435447c331/appId/5fa458dd-3f24-4176-88eb-38277b6c62de
Microsoft Entra admin center
Search resources, services, and docs (G+/)
julian.rasmussen@idefix...
IDEFIX (IDEFIX365.NO)
Home
What's new
Diagnose & solve problems
Favorites
Privileged Identity Management
All users
Identity
Protection
Identity Governance
Verified ID
Permissions Management
Global Secure Access
Dashboard
Applications
Connect
Traffic forwarding
Client download
Remote networks
Connectors
Secure
Monitor
Learn & support
Home > Idefix > Traffic forwarding >
Users and groups
GSA-Microsoft365trafficforwardingprofile
Add user/group
Edit assignment
Remove
Update credentials
Columns
Got feedback?
The application will appear for assigned users within My Apps. Set 'visible to users?' to no in properties to prevent this. →
Assign users and groups to app-roles for your application here. To create new app-roles for this application, use the application registration.
First 200 shown, to search all users & gro...
Display Name
Object Type
Role assigned
DD
Dachshund Dash
User
Default Access

Home
What's new
Diagnose & solve problems
Favorites
Privileged Identity Management
All users
Identity
Protection
Identity Governance
Verified ID
Permissions Management
Global Secure Access
Dashboard
Applications
Connect
Traffic forwarding
Client download
Remote networks
Connectors
Secure
Monitor
Learn & support

Traffic forwarding

Global Secure Access is now in generally available. Licensing requirements have been updated. Licensing enforcement for Microsoft Entra Private Access, Microsoft Entra Inte with General Availability on July 1st, 2024. Learn more

Refresh | Got feedback?

Manage traffic forwarding profiles

Traffic forwarding profiles enable admins to forward specific traffic to Global Secure Access. Assign traffic forwarding profiles to users running the Global Secure Access client. For clientless devices, use the Microsoft profile to assign to remote networks.
Learn more

One or more profiles are configured and ready to use. To finish setup, Download Global Secure Access client.

Microsoft traffic profile

Enabled
Last modified on 10/31/2024, 10:59 PM

Applies to
Internet traffic to Microsoft services

Microsoft traffic policies
3 policies View

Linked Conditional Access policies
2 policies View

User and group assignments
1 users, 0 groups assigned View

Remote network assignments
0 assigned remote networks View

Private access profile

Enabled
Last modified on 10/29/2024, 09:36 PM

Applies to
Private resources

Private access policies
Quick Access, 0 Applications

Linked Conditional Access policies
None

User and group assignments
2 users, 0 groups assigned View

Remote network assignments
Not applicable

Internet access profile

Enabled
Last modified on not available

Applies to
All internet traffic, except for the Microsoft traffic profile

Internet access policies
3 policies View

Linked Conditional Access policies
2 policies View

User and group assignments
2 users, 0 groups assigned View

Remote network assignments
Not applicable

User and group assignments

Microsoft profile

Global Secure Access is now in generally available. Licensing requirements have been updated. Licensing enforcement for Microsoft Entra Private Access, Microsoft Entra Internet Access will begin to rollout on October 1, 2024. This is following a 90-day trial period that began with General Availability on July 1st, 2024. Learn more

Assign users and groups to the traffic forwarding profile. Traffic forwarding profile policies only apply to users assigned to the profile. However, the policies may still apply if a user is on a remote network assigned to the traffic forwarding profile.

Assign to all users No

Select users

Assigned
1 users, 0 groups assigned

Manage traffic forwarding profiles

Traffic forwarding profiles enable admins to forward specific traffic to Global Secure Access. Assign traffic forwarding profiles to users running the Global Secure Access client. For clientless devices, use the Microsoft profile to assign to remote networks.
Learn more

One or more profiles are configured and ready to use. To finish setup, Download Global Secure Access client.

Microsoft traffic profile

Enabled

Last modified on 10/31/2024, 10:59 PM

Applies to
Internet traffic to Microsoft services

Microsoft traffic policies
3 policies View

Linked Conditional Access policies
2 policies View

User and group assignments
1 users, 0 groups assigned View

Remote network assignments
0 assigned remote networks View

Private access profile

Enabled

Last modified on 10/29/2024, 09:36 PM

Applies to
Private resources

Private access policies
Quick Access, 0 Applications

Linked Conditional Access policies
None

User and group assignments
2 users, 0 groups assigned View

Remote network assignments
Not applicable

Internet access profile

Enabled

Last modified on not available

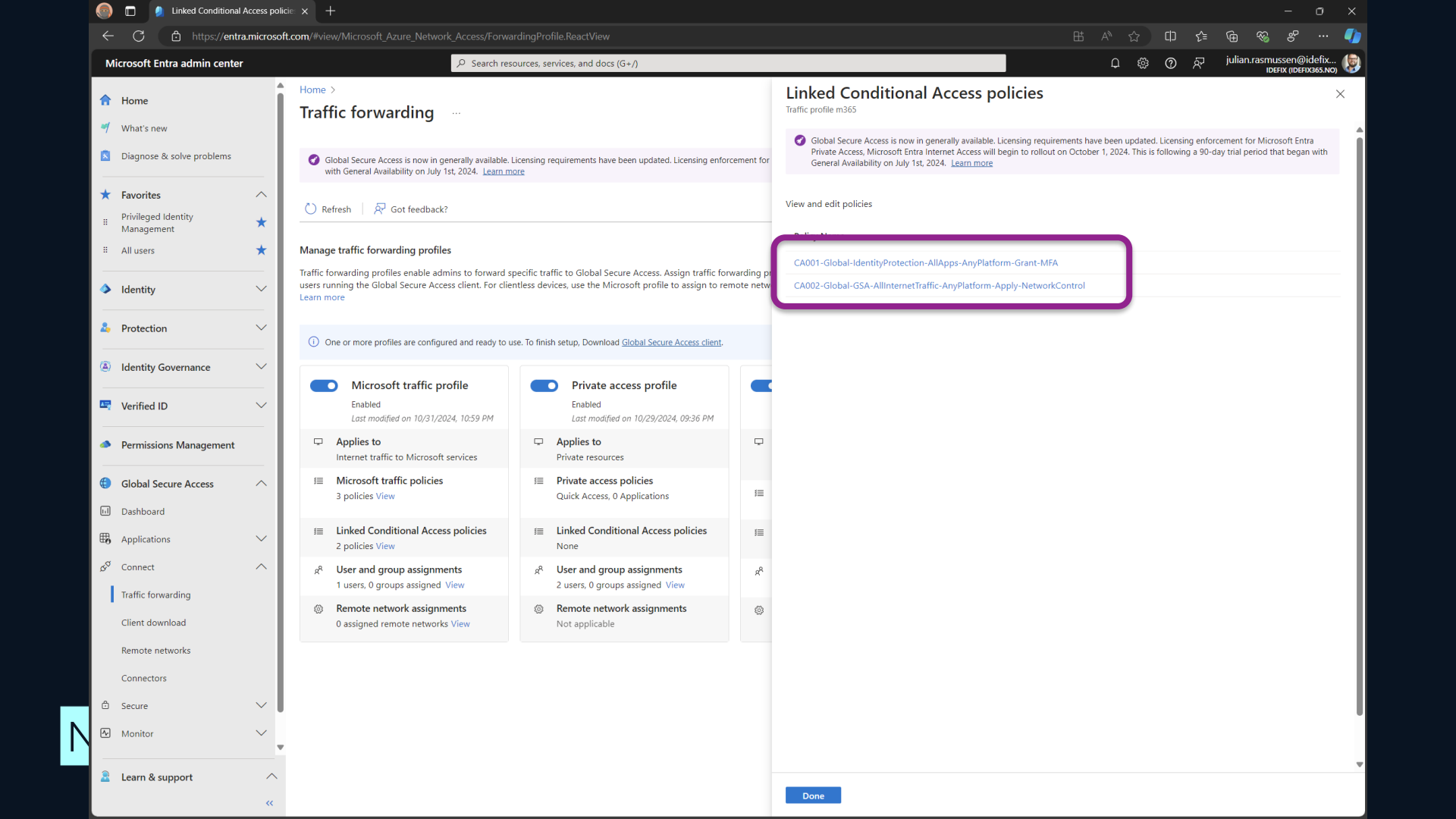
Applies to
All internet traffic, except for the Microsoft traffic profile

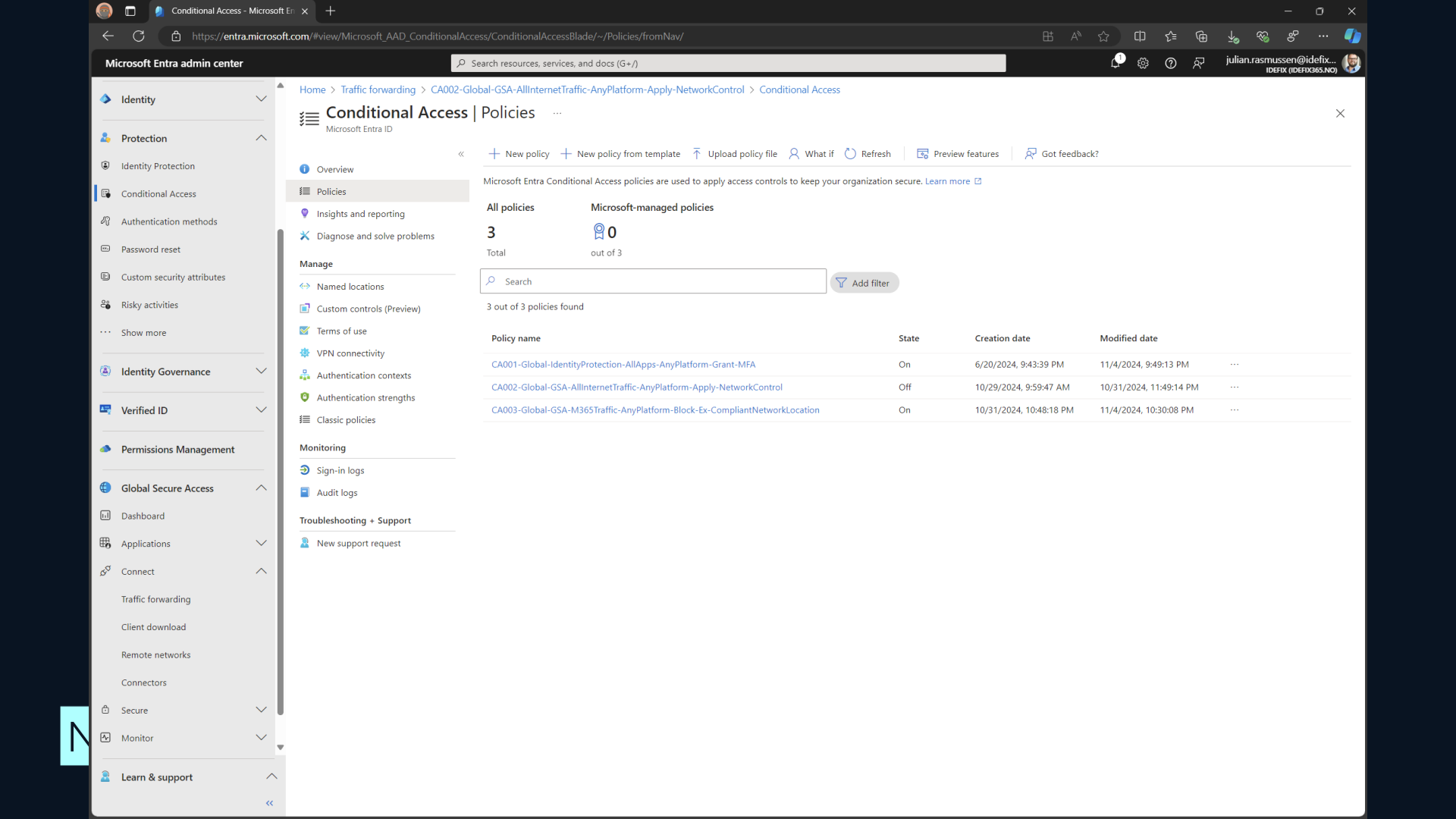
Internet access policies
3 policies View

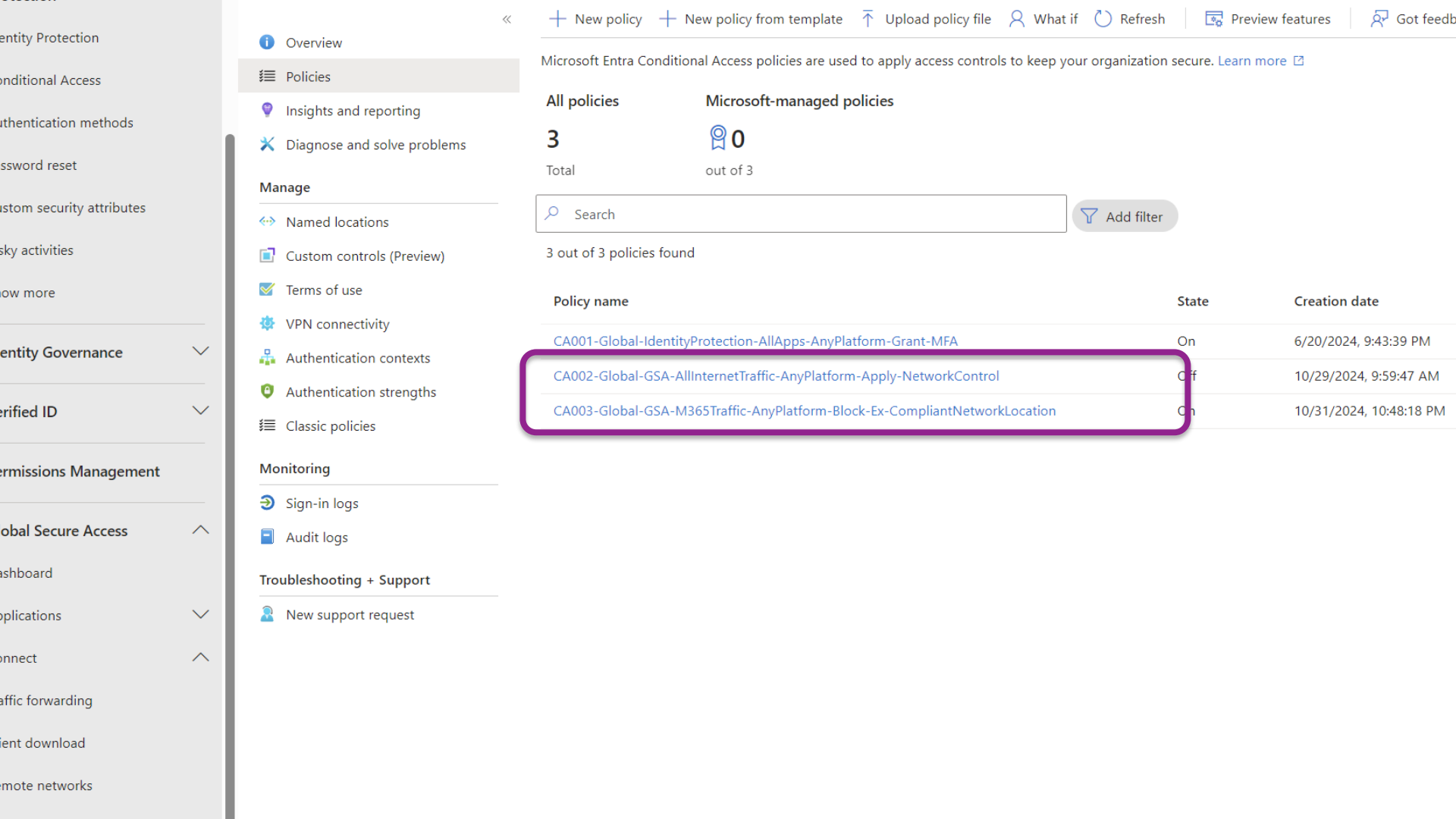
Linked Conditional Access policies
2 policies View

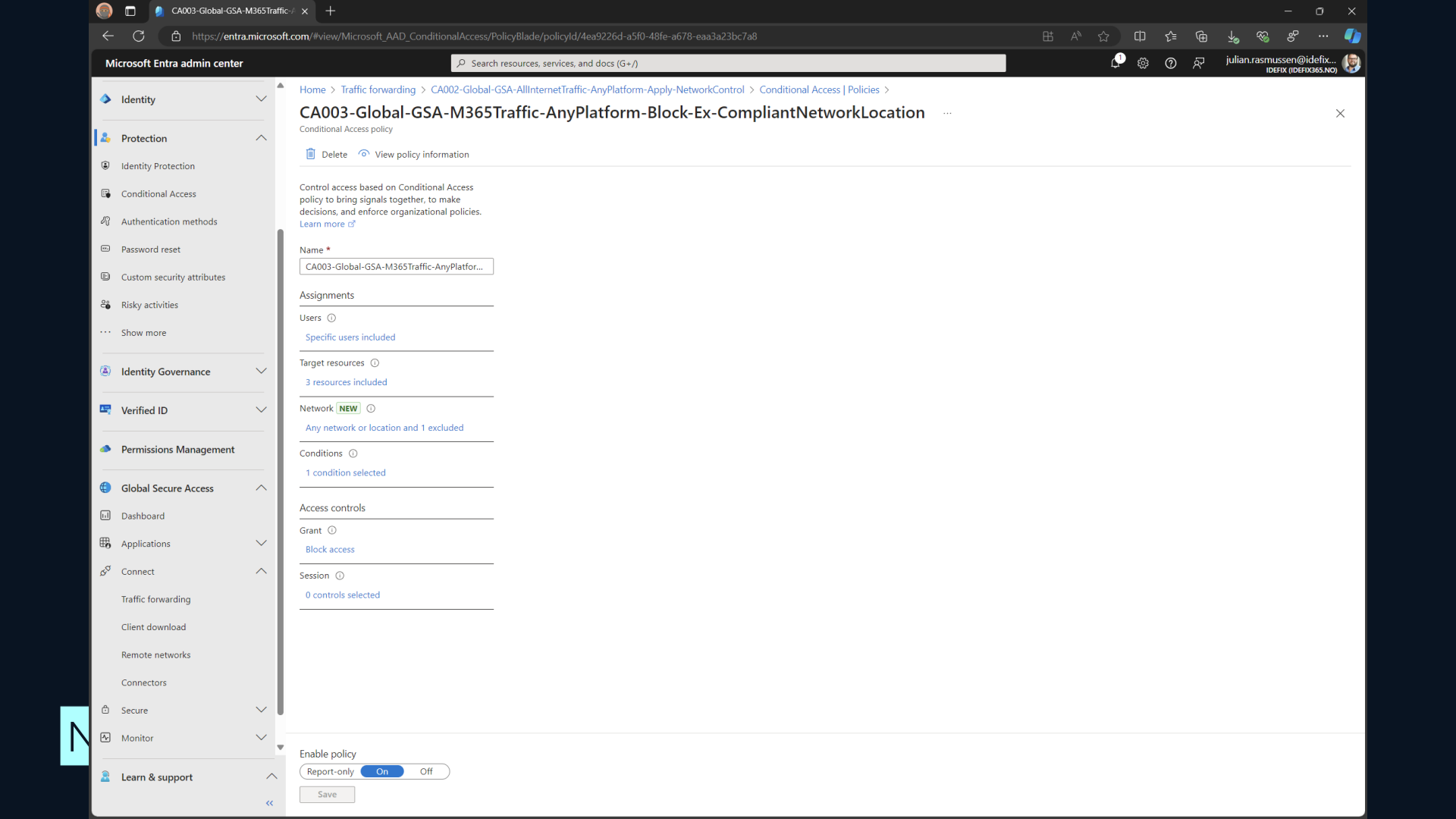
User and group assignments
2 users, 0 groups assigned View

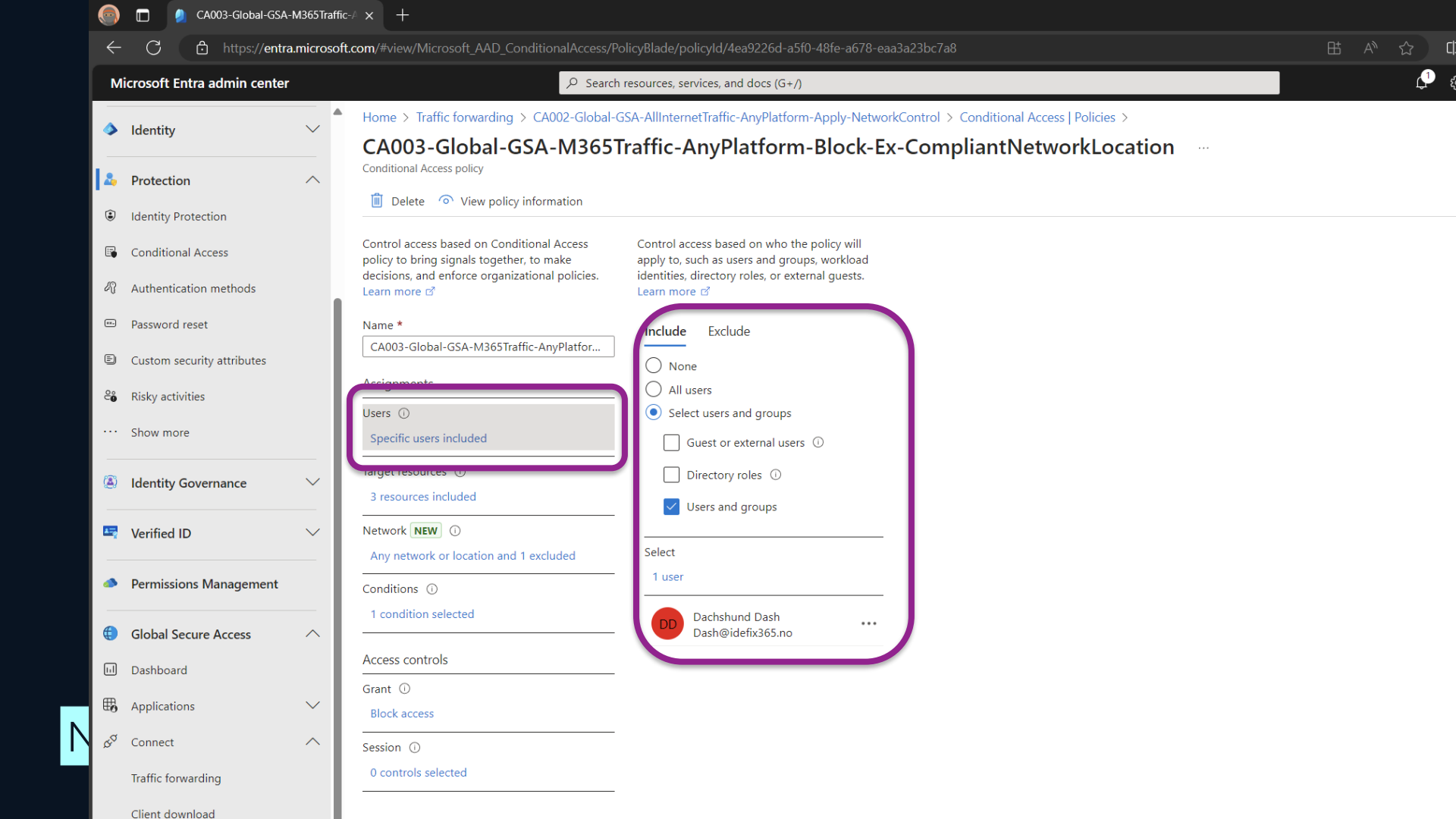
Remote network assignments
Not applicable

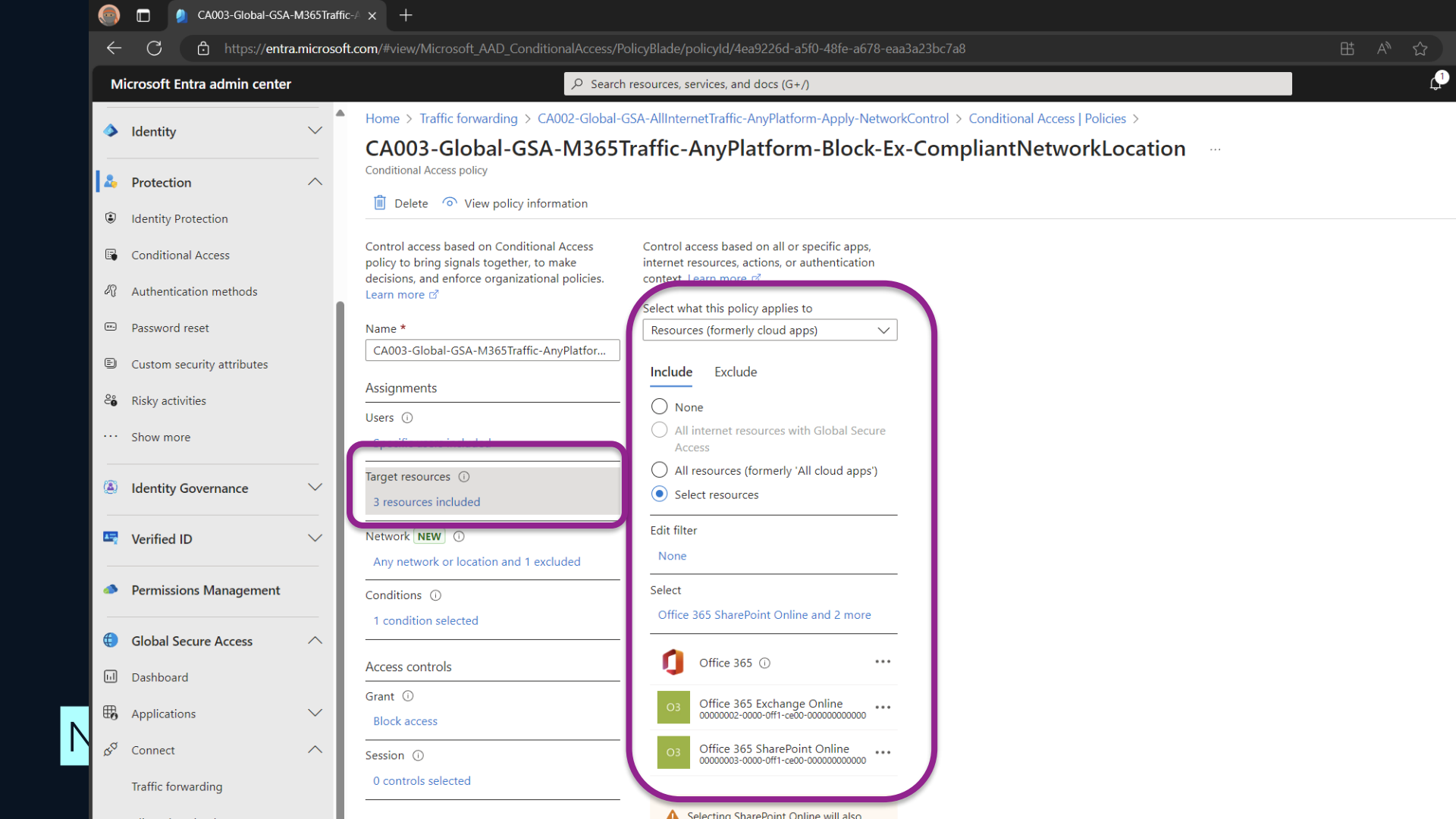

Linked Conditional Access policies
https://entra.microsoft.com/#view/Microsoft_Azure_Network_Access/ForwardingProfile.ReactView
Microsoft Entra admin center
Search resources, services, and docs (G+/)
julian.rasmussen@idefix...
IDEFIX (IDEFIX365.NO)
Home
What's new
Diagnose & solve problems
Favorites
Privileged Identity Management
All users
Identity
Protection
Identity Governance
Verified ID
Permissions Management
Global Secure Access
Dashboard
Applications
Connect
Traffic forwarding
Client download
Remote networks
Connectors
Secure
Monitor
Learn & support
Home >
Traffic forwarding
Global Secure Access is now in generally available. Licensing requirements have been updated. Licensing enforcement for
with General Availability on July 1st, 2024. Learn more
Refresh
Got feedback?
Manage traffic forwarding profiles
Traffic forwarding profiles enable admins to forward specific traffic to Global Secure Access. Assign traffic forwarding p
users running the Global Secure Access client. For clientless devices, use the Microsoft profile to assign to remote netw
Learn more
One or more profiles are configured and ready to use. To finish setup, Download Global Secure Access client.
Microsoft traffic profile
Enabled
Last modified on 10/31/2024, 10:59 PM
Applies to
Internet traffic to Microsoft services
Microsoft traffic policies
3 policies View
Linked Conditional Access policies
2 policies View
User and group assignments
1 users, 0 groups assigned View
Remote network assignments
0 assigned remote networks View
Private access profile
Enabled
Last modified on 10/29/2024, 09:36 PM
Applies to
Private resources
Private access policies
Quick Access, 0 Applications
Linked Conditional Access policies
None
User and group assignments
2 users, 0 groups assigned View
Remote network assignments
Not applicable
Linked Conditional Access policies
Traffic profile m365
Global Secure Access is now in generally available. Licensing requirements have been updated. Licensing enforcement for Microsoft Entra Private Access, Microsoft Entra Internet Access will begin to rollout on October 1, 2024. This is following a 90-day trial period that began with General Availability on July 1st, 2024. Learn more
View and edit policies
CA001-Global-IdentityProtection-AllApps-AnyPlatform-Grant-MFA
CA002-Global-GSA-AllInternetTraffic-AnyPlatform-Apply-NetworkControl
Done

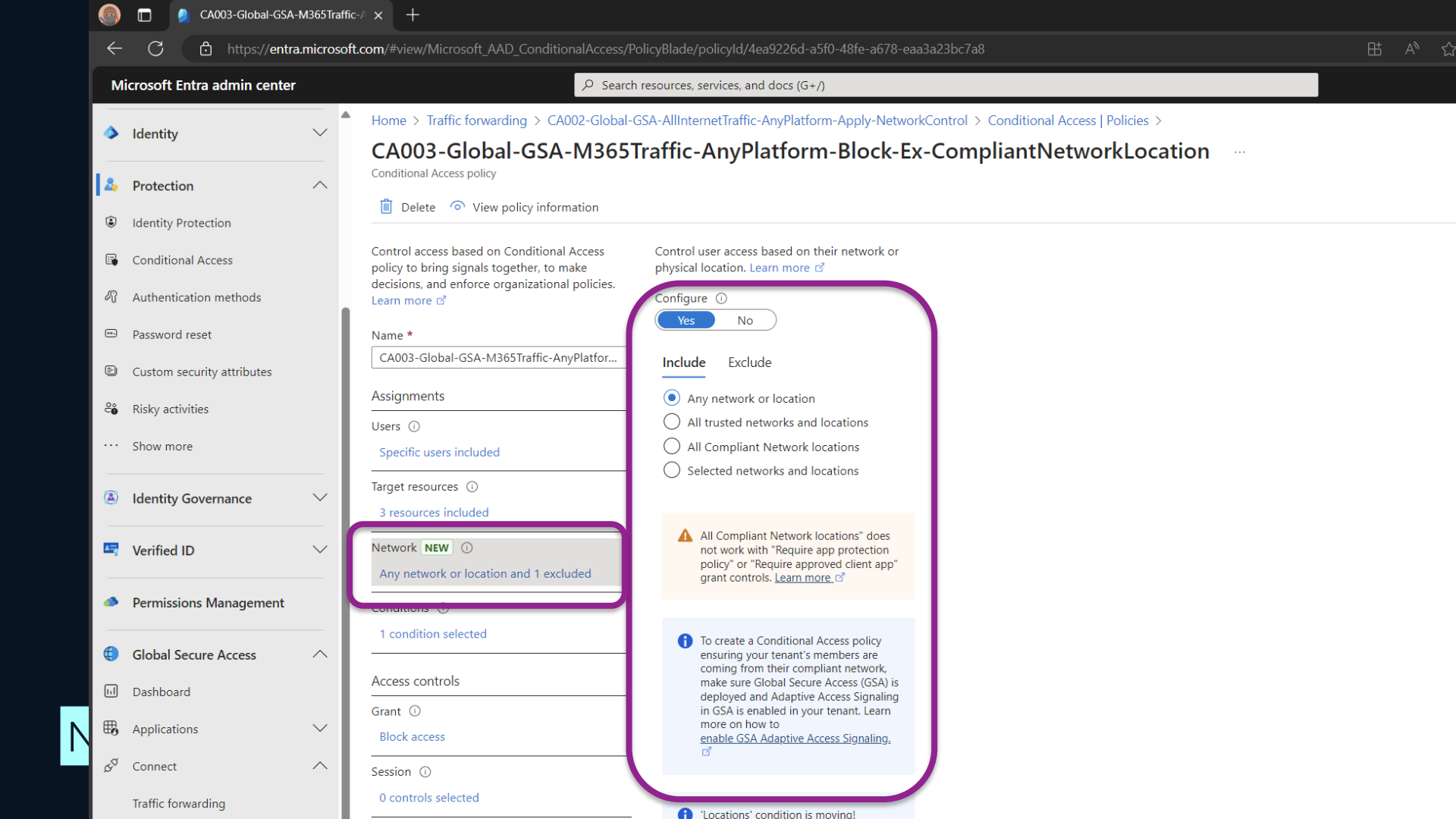

Conditional Access - Microsoft Entra admin center
https://entra.microsoft.com/#view/Microsoft_AAD_ConditionalAccess/ConditionalAccessBlade/~/Policies/fromNav/
Microsoft Entra admin center
Search resources, services, and docs (G+/)
julian.rasmussen@idefix...
IDEFIX (IDEFIX365.NO)
Identity
Protection
Identity Protection
Conditional Access
Authentication methods
Password reset
Custom security attributes
Risky activities
Show more
Identity Governance
Verified ID
Permissions Management
Global Secure Access
Dashboard
Applications
Connect
Traffic forwarding
Client download
Remote networks
Connectors
Secure
Monitor
Learn & support
Home > Traffic forwarding > CA002-Global-GSA-AllInternetTraffic-AnyPlatform-Apply-NetworkControl > Conditional Access
Conditional Access | Policies
Microsoft Entra ID
Overview
Policies
Insights and reporting
Diagnose and solve problems
Manage
Named locations
Custom controls (Preview)
Terms of use
VPN connectivity
Authentication contexts
Authentication strengths
Classic policies
Monitoring
Sign-in logs
Audit logs
Troubleshooting + Support
New support request
New policy
New policy from template
Upload policy file
What if
Refresh
Preview features
Got feedback?
Microsoft Entra Conditional Access policies are used to apply access controls to keep your organization secure. Learn more
All policies
3
Total
Microsoft-managed policies
0
out of 3
Search
Add filter
3 out of 3 policies found
Policy name
State
Creation date
Modified date
CA001-Global-IdentityProtection-AllApps-AnyPlatform-Grant-MFA
On
6/20/2024, 9:43:39 PM
11/4/2024, 9:49:13 PM
CA002-Global-GSA-AllInternetTraffic-AnyPlatform-Apply-NetworkControl
Off
10/29/2024, 9:59:47 AM
10/31/2024, 11:49:14 PM
CA003-Global-GSA-M365Traffic-AnyPlatform-Block-Ex-CompliantNetworkLocation
On
10/31/2024, 10:48:18 PM
11/4/2024, 10:30:08 PM

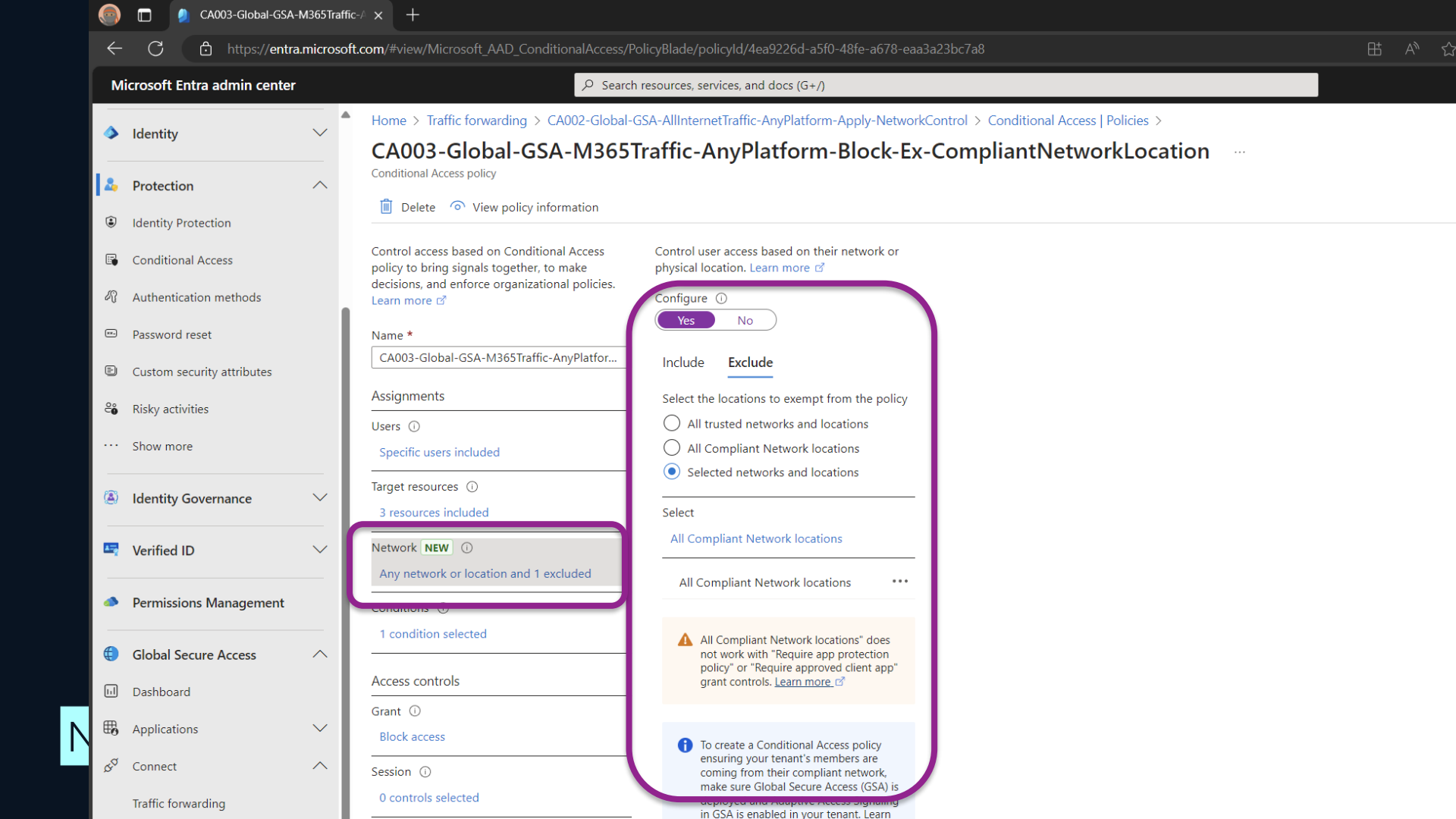

ntity Protection
nditional Access
thentication methods
ssword reset
stom security attributes
sky activities
ow more
ntity Governance
rified ID
rmissions Management
obal Secure Access
shboard
plications
nnect
affic forwarding
ient download
mote networks
Overview
Policies
Insights and reporting
Diagnose and solve problems
Manage
Named locations
Custom controls (Preview)
Terms of use
VPN connectivity
Authentication contexts
Authentication strengths
Classic policies
Monitoring
Sign-in logs
Audit logs
Troubleshooting + Support
New support request
New policy
New policy from template
Upload policy file
What if
Refresh
Preview features
Got feedb
Microsoft Entra Conditional Access policies are used to apply access controls to keep your organization secure. Learn more
All policies
3
Total
Microsoft-managed policies
0
out of 3
Search
Add filter
3 out of 3 policies found
Policy name
State
Creation date
CA001-Global-IdentityProtection-AllApps-AnyPlatform-Grant-MFA
On
6/20/2024, 9:43:39 PM
CA002-Global-GSA-AllInternetTraffic-AnyPlatform-Apply-NetworkControl
Off
10/29/2024, 9:59:47 AM
CA003-Global-GSA-M365Traffic-AnyPlatform-Block-Ex-CompliantNetworkLocation
On
10/31/2024, 10:48:18 PM


CA003-Global-GSA-M365Traffic-
https://entra.microsoft.com/#view/Microsoft_AAD_ConditionalAccess/PolicyBlade/policyId/4ea9226d-a5f0-48fe-a678-eaa3a23bc7a8
Microsoft Entra admin center
Search resources, services, and docs (G+/)
julian.rasmussen@idefix...
IDEFIX (IDEFIX365.NO)
Identity
Protection
Identity Protection
Conditional Access
Authentication methods
Password reset
Custom security attributes
Risky activities
Show more
Identity Governance
Verified ID
Permissions Management
Global Secure Access
Dashboard
Applications
Connect
Traffic forwarding
Client download
Remote networks
Connectors
Secure
Monitor
Learn & support
Home > Traffic forwarding > CA002-Global-GSA-AllInternetTraffic-AnyPlatform-Apply-NetworkControl > Conditional Access | Policies >
CA003-Global-GSA-M365Traffic-AnyPlatform-Block-Ex-CompliantNetworkLocation
Conditional Access policy
Delete
View policy information
Control access based on Conditional Access policy to bring signals together, to make decisions, and enforce organizational policies.
Learn more
Name *
CA003-Global-GSA-M365Traffic-AnyPlatfor...
Assignments
Users
Specific users included
Target resources
3 resources included
Network NEW
Any network or location and 1 excluded
Conditions
1 condition selected
Access controls
Grant
Block access
Session
0 controls selected
Enable policy
Report-only
On
Off
Save


CA003-Global-GSA-M365Traffic-A
https://entra.microsoft.com/#view/Microsoft_AAD_ConditionalAccess/PolicyBlade/policyId/4ea9226d-a5f0-48fe-a678-eaa3a23bc7a8
Microsoft Entra admin center
Search resources, services, and docs (G+/)
Identity
Protection
Identity Protection
Conditional Access
Authentication methods
Password reset
Custom security attributes
Risky activities
Show more
Identity Governance
Verified ID
Permissions Management
Global Secure Access
Dashboard
Applications
Connect
Traffic forwarding
Client download
Home > Traffic forwarding > CA002-Global-GSA-AllInternetTraffic-AnyPlatform-Apply-NetworkControl > Conditional Access | Policies >
CA003-Global-GSA-M365Traffic-AnyPlatform-Block-Ex-CompliantNetworkLocation
Conditional Access policy
Delete
View policy information
Control access based on Conditional Access policy to bring signals together, to make decisions, and enforce organizational policies.
Learn more
Name *
CA003-Global-GSA-M365Traffic-AnyPlatfor...
Assignments
Users
Specific users included
Target resources
3 resources included
Network NEW
Any network or location and 1 excluded
Conditions
1 condition selected
Access controls
Grant
Block access
Session
0 controls selected
Control access based on who the policy will apply to, such as users and groups, workload identities, directory roles, or external guests.
Learn more
Include
Exclude
None
All users
Select users and groups
Guest or external users
Directory roles
Users and groups
Select
1 user
DD
Dachshund Dash
Dash@idefix365.no


CA003-Global-GSA-M365Traffic-
https://entra.microsoft.com/#view/Microsoft_AAD_ConditionalAccess/PolicyBlade/policyId/4ea9226d-a5f0-48fe-a678-eaa3a23bc7a8
Microsoft Entra admin center
Search resources, services, and docs (G+/)
Identity
Protection
Identity Protection
Conditional Access
Authentication methods
Password reset
Custom security attributes
Risky activities
Show more
Identity Governance
Verified ID
Permissions Management
Global Secure Access
Dashboard
Applications
Connect
Traffic forwarding
Home > Traffic forwarding > CA002-Global-GSA-AllInternetTraffic-AnyPlatform-Apply-NetworkControl > Conditional Access | Policies >
CA003-Global-GSA-M365Traffic-AnyPlatform-Block-Ex-CompliantNetworkLocation
Conditional Access policy
Delete
View policy information
Control access based on Conditional Access policy to bring signals together, to make decisions, and enforce organizational policies. Learn more
Name *
CA003-Global-GSA-M365Traffic-AnyPlatfor...
Assignments
Users
Target resources
3 resources included
Network NEW
Any network or location and 1 excluded
Conditions
1 condition selected
Access controls
Grant
Block access
Session
0 controls selected
Control access based on all or specific apps, internet resources, actions, or authentication context. Learn more
Select what this policy applies to
Resources (formerly cloud apps)
Include
Exclude
None
All internet resources with Global Secure Access
All resources (formerly 'All cloud apps')
Select resources
Edit filter
None
Select
Office 365 SharePoint Online and 2 more
Office 365
Office 365 Exchange Online
00000002-0000-0ff1-ce00-000000000000
Office 365 SharePoint Online
00000003-0000-0ff1-ce00-000000000000


CA003-Global-GSA-M365Traffic-A
https://entra.microsoft.com/#view/Microsoft_AAD_ConditionalAccess/PolicyBlade/policyId/4ea9226d-a5f0-48fe-a678-eaa3a23bc7a8
Microsoft Entra admin center
Search resources, services, and docs (G+/)
Identity
Protection
Identity Protection
Conditional Access
Authentication methods
Password reset
Custom security attributes
Risky activities
Show more
Identity Governance
Verified ID
Permissions Management
Global Secure Access
Dashboard
Applications
Connect
Traffic forwarding
Home > Traffic forwarding > CA002-Global-GSA-AllInternetTraffic-AnyPlatform-Apply-NetworkControl > Conditional Access | Policies >
CA003-Global-GSA-M365Traffic-AnyPlatform-Block-Ex-CompliantNetworkLocation
Conditional Access policy
Delete
View policy information
Control access based on Conditional Access policy to bring signals together, to make decisions, and enforce organizational policies. Learn more
Name *
CA003-Global-GSA-M365Traffic-AnyPlatfor...
Assignments
Users
Specific users included
Target resources
3 resources included
Network NEW
Any network or location and 1 excluded
1 condition selected
Access controls
Grant
Block access
Session
0 controls selected
Control user access based on their network or physical location. Learn more
Configure
Yes
No
Include
Exclude
Any network or location
All trusted networks and locations
All Compliant Network locations
Selected networks and locations
All Compliant Network locations" does not work with "Require app protection policy" or "Require approved client app" grant controls. Learn more
To create a Conditional Access policy ensuring your tenant's members are coming from their compliant network, make sure Global Secure Access (GSA) is deployed and Adaptive Access Signaling in GSA is enabled in your tenant. Learn more on how to enable GSA Adaptive Access Signaling.
'Locations' condition is moving!


CA003-Global-GSA-M365Traffic-A
https://entra.microsoft.com/#view/Microsoft_AAD_ConditionalAccess/PolicyBlade/policyId/4ea9226d-a5f0-48fe-a678-eaa3a23bc7a8
Microsoft Entra admin center
Search resources, services, and docs (G+/)
Identity
Protection
Identity Protection
Conditional Access
Authentication methods
Password reset
Custom security attributes
Risky activities
Show more
Identity Governance
Verified ID
Permissions Management
Global Secure Access
Dashboard
Applications
Connect
Traffic forwarding
Home > Traffic forwarding > CA002-Global-GSA-AllInternetTraffic-AnyPlatform-Apply-NetworkControl > Conditional Access | Policies >
CA003-Global-GSA-M365Traffic-AnyPlatform-Block-Ex-CompliantNetworkLocation
Conditional Access policy
Delete
View policy information
Control access based on Conditional Access policy to bring signals together, to make decisions, and enforce organizational policies. Learn more
Name *
CA003-Global-GSA-M365Traffic-AnyPlatfor...
Assignments
Users
Specific users included
Target resources
3 resources included
Network NEW
Any network or location and 1 excluded
1 condition selected
Access controls
Grant
Block access
Session
0 controls selected
Control user access based on their network or physical location. Learn more
Configure
Yes
No
Include
Exclude
Select the locations to exempt from the policy
All trusted networks and locations
All Compliant Network locations
Selected networks and locations
Select
All Compliant Network locations
All Compliant Network locations
All Compliant Network locations" does not work with "Require app protection policy" or "Require approved client app" grant controls. Learn more
To create a Conditional Access policy ensuring your tenant's members are coming from their compliant network, make sure Global Secure Access (GSA) is
in GSA is enabled in your tenant. Learn

CA003-Global-GSA-M365Traffic-AnyPlatform-Block-Ex-CompliantNetworkLocation

Conditional Access policy

Delete | View policy information

Control access based on Conditional Access policy to bring signals together, to make decisions, and enforce organizational policies.
Learn more

Name *
CA003-Global-GSA-M365Traffic-AnyPlatfor...

Assignments

Users
Specific users included

Target resources
3 resources included

Network NEW
Any network or location and 1 excluded

Conditions
1 condition selected

Access controls

Grant
Block access

Session
0 controls selected

Grant

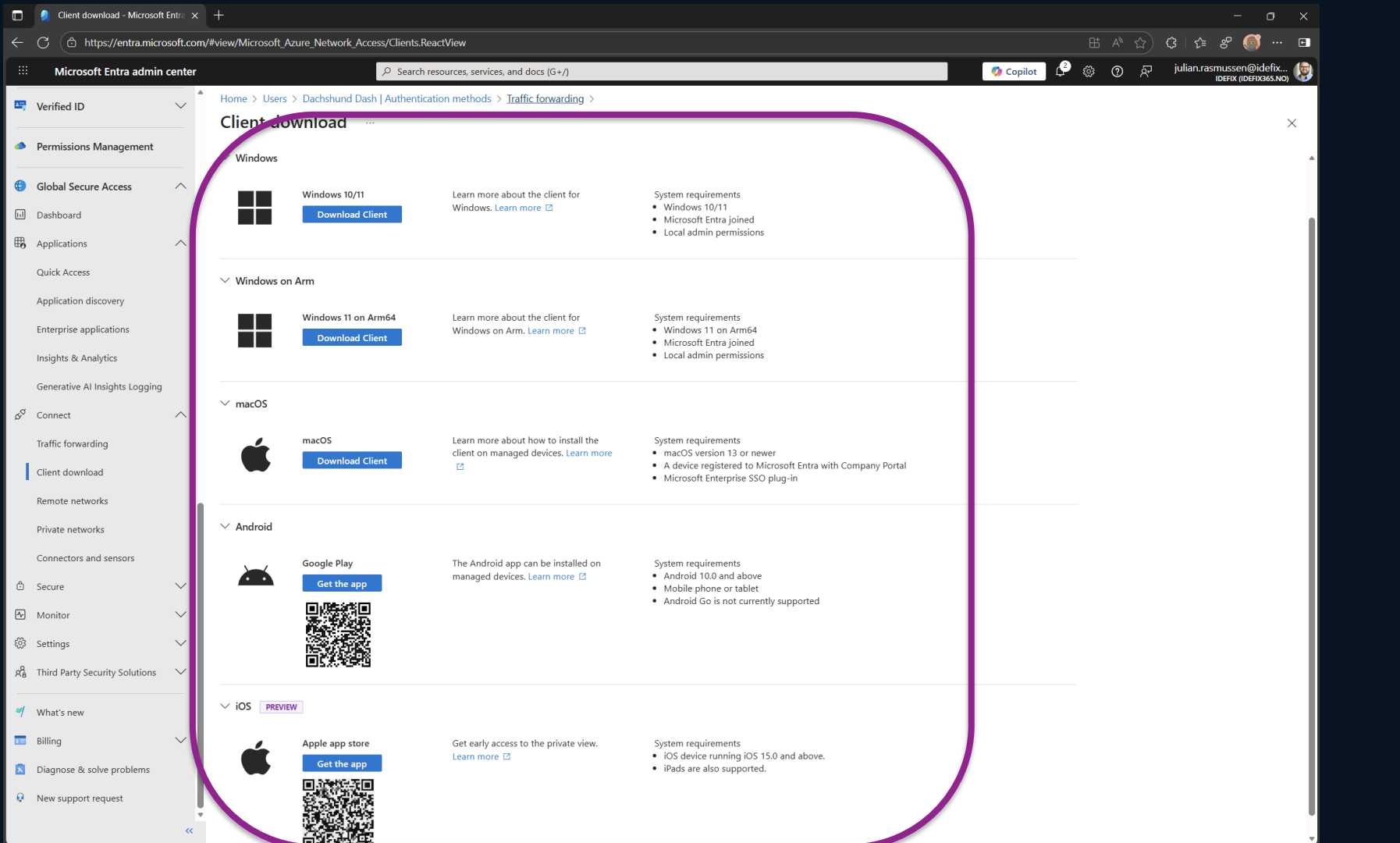
Control access enforcement to block or grant access. Learn more

- (•) Block access
- ( ) Grant access

- [ ] Require multifactor authentication
- [ ] Require authentication strength
- [ ] Require device to be marked as compliant
- [ ] Require Microsoft Entra hybrid joined device
- [ ] Require approved client app
  See list of approved client apps
- [ ] Require app protection policy
  See list of policy protected client apps
- [ ] Require password change

For multiple controls

- ( ) Require all the selected controls
- (•) Require one of the selected controls


Client download - Microsoft Entra
https://entra.microsoft.com/#view/Microsoft_Azure_Network_Access/Clients.ReactView
Microsoft Entra admin center
Search resources, services, and docs (G+/)
Copilot
julian.rasmussen@idefix...
IDEFIX (IDEFIX365.NO)
Verified ID
Permissions Management
Global Secure Access
Dashboard
Applications
Quick Access
Application discovery
Enterprise applications
Insights & Analytics
Generative AI Insights Logging
Connect
Traffic forwarding
Client download
Remote networks
Private networks
Connectors and sensors
Secure
Monitor
Settings
Third Party Security Solutions
What's new
Billing
Diagnose & solve problems
New support request
Home > Users > Dachshund Dash | Authentication methods > Traffic forwarding >
Client download
Windows
Windows 10/11
Download Client
Learn more about the client for Windows. Learn more
System requirements
Windows 10/11
Microsoft Entra joined
Local admin permissions
Windows on Arm
Windows 11 on Arm64
Download Client
Learn more about the client for Windows on Arm. Learn more
System requirements
Windows 11 on Arm64
Microsoft Entra joined
Local admin permissions
macOS
macOS
Download Client
Learn more about how to install the client on managed devices. Learn more
System requirements
macOS version 13 or newer
A device registered to Microsoft Entra with Company Portal
Microsoft Enterprise SSO plug-in
Android
Google Play
Get the app
The Android app can be installed on managed devices. Learn more
System requirements
Android 10.0 and above
Mobile phone or tablet
Android Go is not currently supported
iOS
PREVIEW
Apple app store
Get the app
Get early access to the private view. Learn more
System requirements
iOS device running iOS 15.0 and above.
iPads are also supported.

Demo SharePoint Access

NIC REBEL EDITION

Demo Blocked SharePoint Access

NIC REBEL EDITION

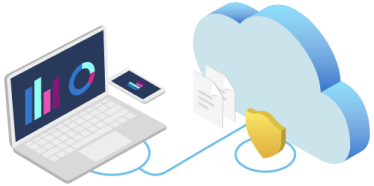
Demo of setup for Internet Traffic

NIC REBEL EDITION

Protection
Identity Protection
Conditional Access
Authentication methods
Password reset
Custom security attributes
Risky activities
Show more
Identity Governance
Verified ID
Permissions Management
Global Secure Access
Dashboard
Applications
Connect
Traffic forwarding
Client download
Remote networks
Connectors
Secure
Monitor
Settings
Learn & support

Idefix

Global Secure Access is now in generally available. Licensing requirements have been updated. Licensing enforcement for Microsoft Entra Private Access, Microsoft Entra Internet Access will begin to rollout on October 1, 2024. This is following a 90-day trial period that began with General Availability on July 1st, 2024. Learn more



Welcome to Global Secure Access

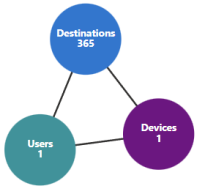
Secure access and improve visibility to the internet, Microsoft 365, SaaS, and private apps. Learn more about Global Secure Access

Get Started with the dashboard | Got feedback?

Last 24 hours

Global Secure Access snapshot

Traffic type : All



The Global Secure Access snapshots provides quick access to the users, devices, and destinations with network traffic captured by Microsoft Entra Private Access and Microsoft Entra Internet Access.

Out of 10 devices, 1 have the Global Secure Access Client installed: 10.0%

Device status

Active devices

1 ▲ 0% in the last 24 hours

The number of distinct active devices that signed in to other tenants in the last 24 hours

Alerts and notifications PREVIEW

No notifications in the last 24 hours

You're up to date

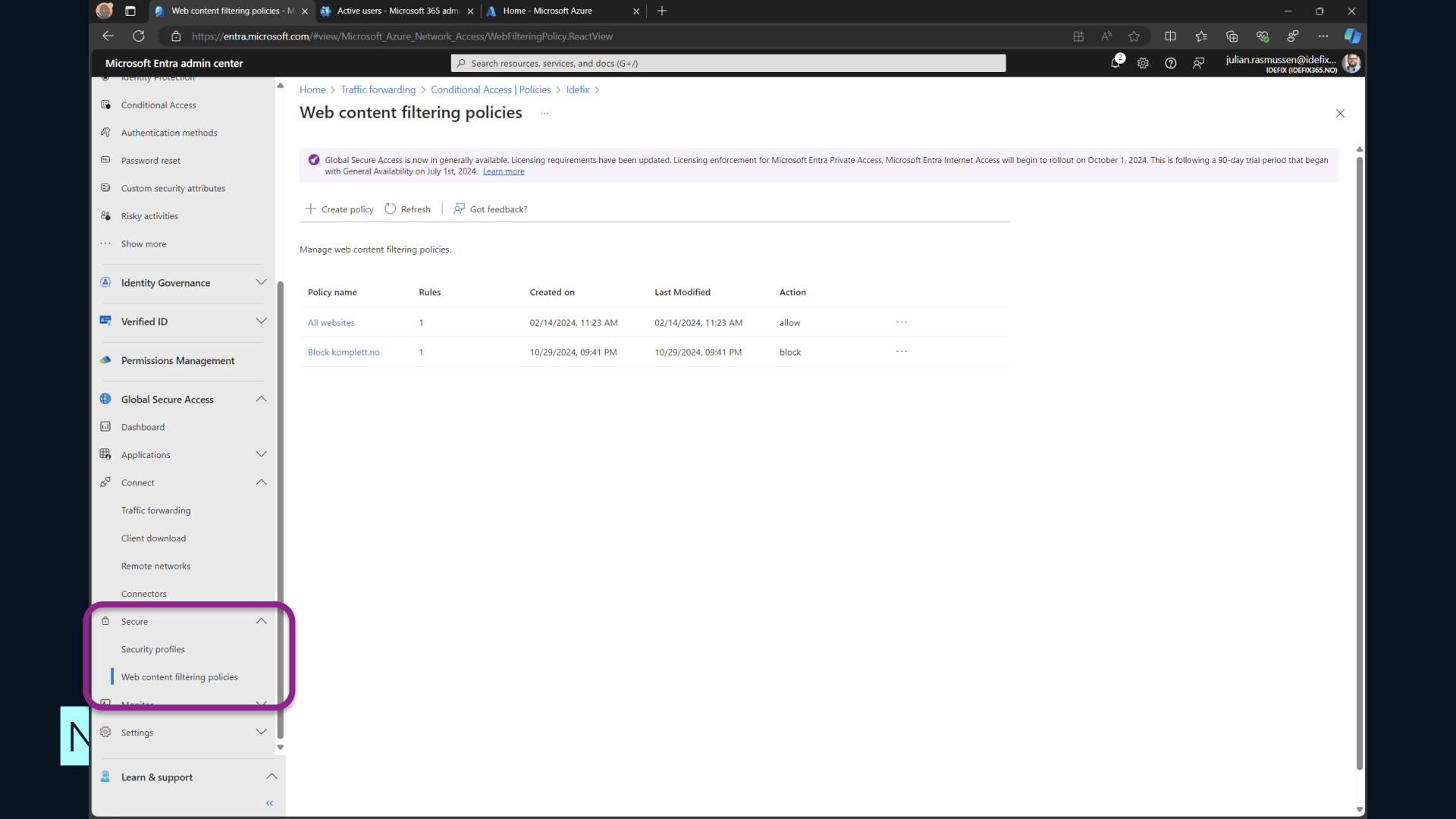
Top used destinations

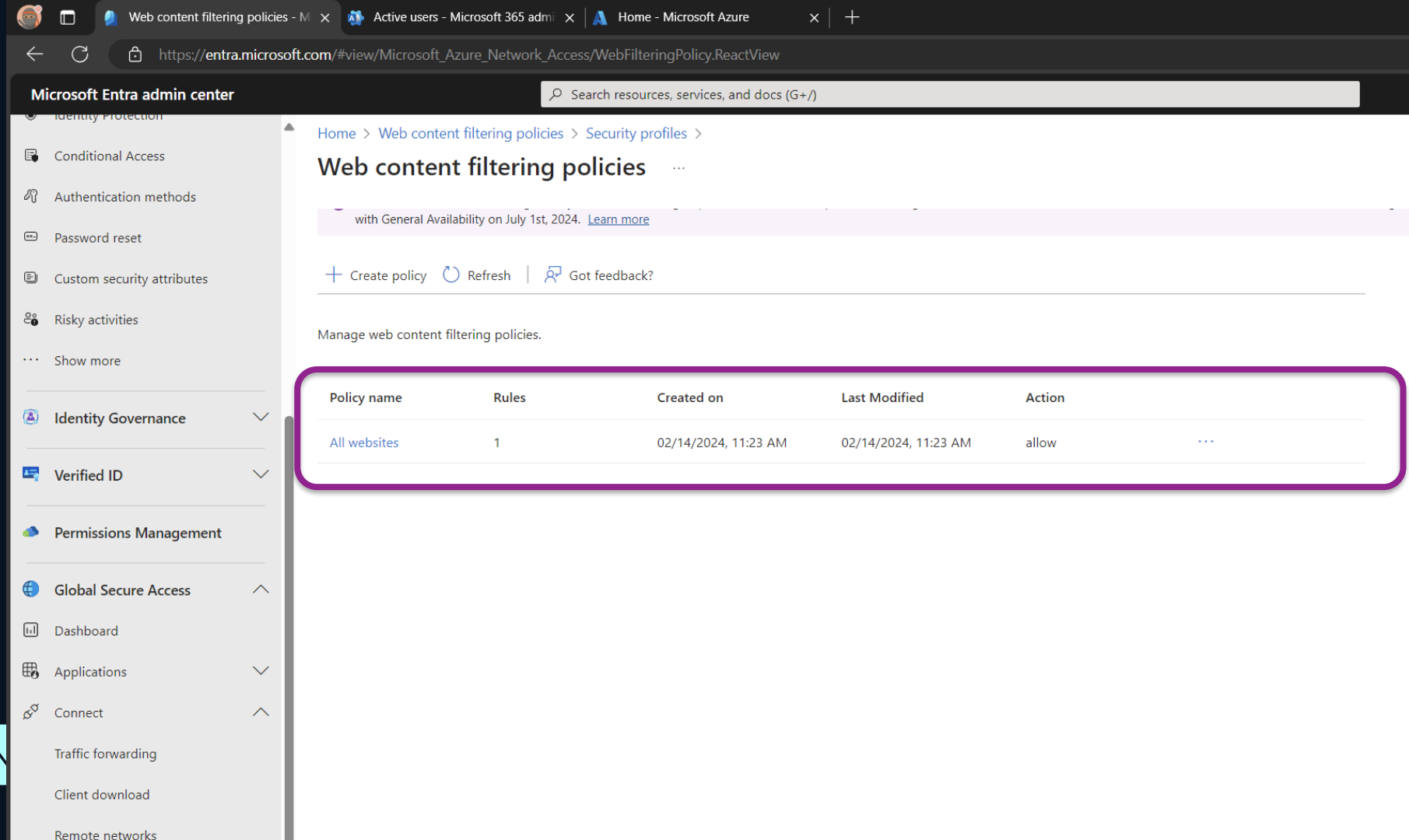
Review the top-used destinations by traffic type.

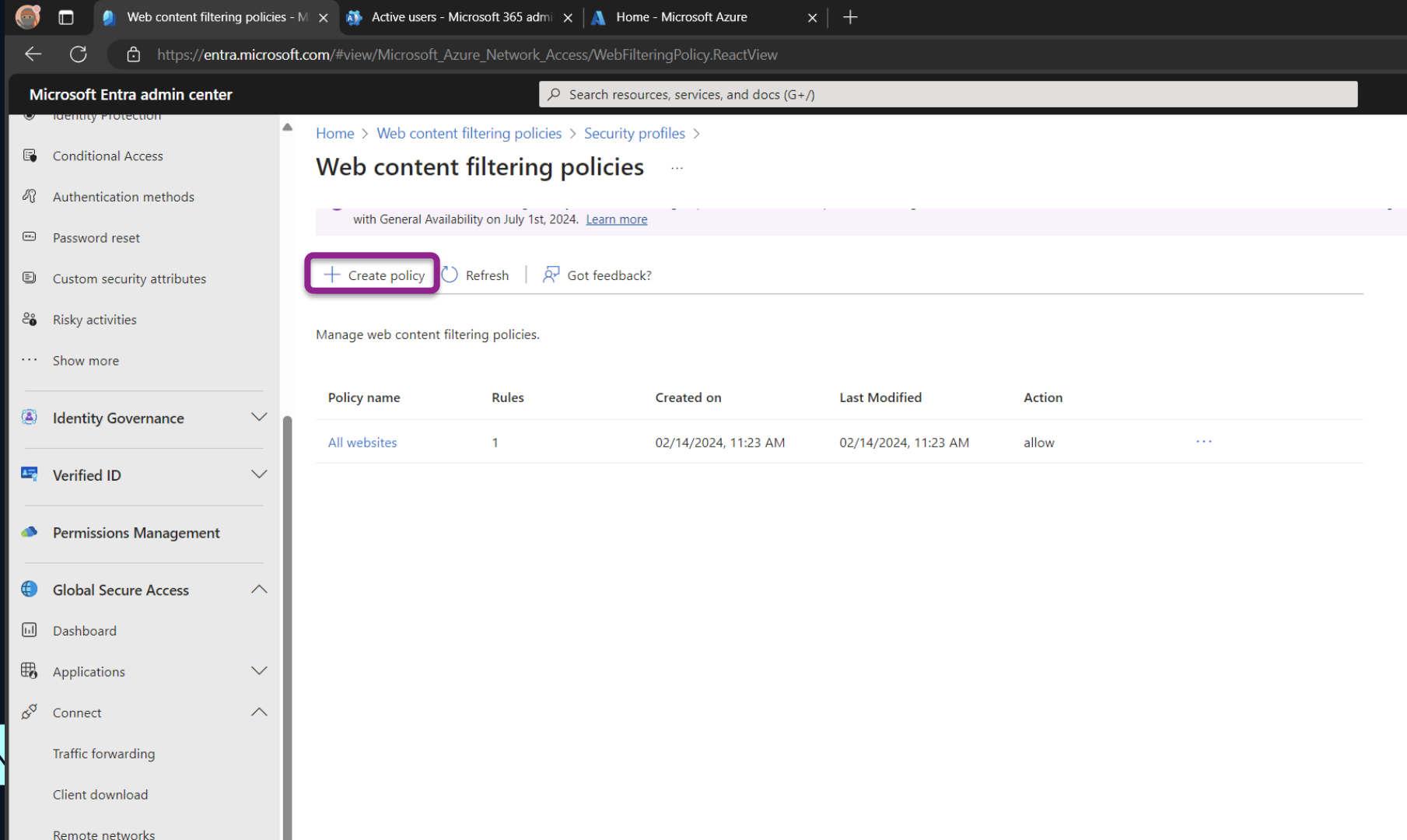
All | Microsoft 365 | Internet Access | Private Access

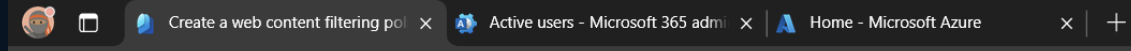
Sort by : Transactions

westeurope-shared.prod.warm.ingest.monitor.core.windows.net 13K


Web content filtering policies - M
Active users - Microsoft 365 admi
Home - Microsoft Azure
https://entra.microsoft.com/#view/Microsoft_Azure_Network_Access/WebFilteringPolicy.ReactView
Microsoft Entra admin center
Search resources, services, and docs (G+/)
julian.rasmussen@idefix...
IDEFIX (IDEFIX365.NO)
Conditional Access
Authentication methods
Password reset
Custom security attributes
Risky activities
Show more
Identity Governance
Verified ID
Permissions Management
Global Secure Access
Dashboard
Applications
Connect
Traffic forwarding
Client download
Remote networks
Connectors
Secure
Security profiles
Web content filtering policies
Settings
Learn & support
Home > Traffic forwarding > Conditional Access | Policies > Idefix >
Web content filtering policies
Global Secure Access is now in generally available. Licensing requirements have been updated. Licensing enforcement for Microsoft Entra Private Access, Microsoft Entra Internet Access will begin to rollout on October 1, 2024. This is following a 90-day trial period that began with General Availability on July 1st, 2024. Learn more
Create policy
Refresh
Got feedback?
Manage web content filtering policies.
Policy name
Rules
Created on
Last Modified
Action
All websites
1
02/14/2024, 11:23 AM
02/14/2024, 11:23 AM
allow
Block komplett.no
1
10/29/2024, 09:41 PM
10/29/2024, 09:41 PM
block


Web content filtering policies - M
Active users - Microsoft 365 admi
Home - Microsoft Azure
https://entra.microsoft.com/#view/Microsoft_Azure_Network_Access/WebFilteringPolicy.ReactView
Microsoft Entra admin center
Search resources, services, and docs (G+/)
Conditional Access
Authentication methods
Password reset
Custom security attributes
Risky activities
Show more
Identity Governance
Verified ID
Permissions Management
Global Secure Access
Dashboard
Applications
Connect
Traffic forwarding
Client download
Remote networks
Home > Web content filtering policies > Security profiles >
Web content filtering policies
with General Availability on July 1st, 2024. Learn more
Create policy
Refresh
Got feedback?
Manage web content filtering policies.
Policy name
Rules
Created on
Last Modified
Action
All websites
1
02/14/2024, 11:23 AM
02/14/2024, 11:23 AM
allow


Web content filtering policies - M
Active users - Microsoft 365 admi
Home - Microsoft Azure
https://entra.microsoft.com/#view/Microsoft_Azure_Network_Access/WebFilteringPolicy.ReactView
Microsoft Entra admin center
Search resources, services, and docs (G+/)
Conditional Access
Authentication methods
Password reset
Custom security attributes
Risky activities
Show more
Identity Governance
Verified ID
Permissions Management
Global Secure Access
Dashboard
Applications
Connect
Traffic forwarding
Client download
Remote networks
Home > Web content filtering policies > Security profiles >
Web content filtering policies
with General Availability on July 1st, 2024. Learn more
Create policy
Refresh
Got feedback?
Manage web content filtering policies.
Policy name
Rules
Created on
Last Modified
Action
All websites
1
02/14/2024, 11:23 AM
02/14/2024, 11:23 AM
allow



https://entra.microsoft.com/#view/Microsoft_Azure_Network_Access/AddFilteringPolicy.ReactView

Microsoft Entra admin center

Search resources, services, and docs (G+/)

- Identity Protection
- Conditional Access
- Authentication methods
- Password reset
- Custom security attributes
- Risky activities
- Show more
- Identity Governance
- Verified ID
- Permissions Management
- Global Secure Access
  - Dashboard
  - Applications
  - Connect
    - Traffic forwarding
    - Client download

Home > Web content filtering policies > Security profiles > Web content filtering policies >

Create a web content filtering policy

Global Secure Access is now in generally available. Licensing requirements have been updated. Licensing enforcement for Microsoft Entra Private Access, Microsoft Entra Internet Access will b
with General Availability on July 1st, 2024. Learn more

Basics | Policy Rules | Review

Create a new web content filtering policy for your organization. The policy will have a name like "Block Sports Websites".

Name* Block komplett.no

Description Content filter for blocking komplett.no websites

Action* Block

Active users - Microsoft 365 admi | Home - Microsoft Azure

m/#view/Microsoft_Azure_Network_Access/AddFilteringPolicy.ReactView

Search resources, services, and docs (G+/)

julian.rasmussen@idefix...
IDEFIX (IDEFIX365.NO)

Home > Web content filtering policies > Security profiles > Web content filtering policies >

Create a web content filtering policy

Global Secure Access is now in generally available. Licensing requirements have been updated. Licensing enforcement for Microsoft Entra Private Access, Microsoft Entra Inte
with General Availability on July 1st, 2024. Learn more

Basics | Policy Rules | Review

Manage rules in your policy.

+ Add Rule

Name	Destination type	Destination

Add Rule

Global Secure Access is now in generally available. Licensing requirements have been updated. Licensing enforcement for Microsoft Entra Private Access, Microsoft Entra Internet Access will begin to rollout on October 1, 2024. This is following a 90-day trial period that began with General Availability on July 1st, 2024. Learn more

Add a rule to your policy.

Name*

Destination type* webCategory

- webCategory
- fqdn

Search

Search

- Alcohol And Tobacco
  Liability
- Child Abuse Images
  Liability
- Criminal Activity
  Liability
- Dating And Personals
  Liability

Selected items

No items selected

Active users - Microsoft 365 admi | Home - Microsoft Azure

m/#view/Microsoft_Azure_Network_Access/AddFilteringPolicy.ReactView

Search resources, services, and docs (G+/)

julian.rasmussen@idefix...
IDEFIX (IDEFIX365.NO)

Home > Web content filtering policies > Security profiles > Web content filtering policies >

Create a web content filtering policy

Global Secure Access is now in generally available. Licensing requirements have been updated. Licensing enforcement for Microsoft Entra Private Access, Microsoft Entra Inte
with General Availability on July 1st, 2024. Learn more

Basics | Policy Rules | Review

Manage rules in your policy.

+ Add Rule

Name	Destination type	Destination

Add Rule

Global Secure Access is now in generally available. Licensing requirements have been updated. Licensing enforcement for Microsoft Entra Private Access, Microsoft Entra Internet Access will begin to rollout on October 1, 2024. This is following a 90-day trial period that began with General Availability on July 1st, 2024. Learn more

Add a rule to your policy.

Name* block komplett.no

Destination type* fqdn

Destination* *.komplett.no

Conditional Access
Authentication methods
Password reset
Custom security attributes
Risky activities
Show more
Identity Governance
Verified ID
Permissions Management
Global Secure Access
Dashboard
Applications
Connect
Traffic forwarding
Client download
Remote networks
Connectors
Secure
Security profiles
Web content filtering policies
Monitor
Settings
Learn & support

Create a web content filtering policy

Global Secure Access is now in generally available. Licensing requirements have been updated. Licensing enforcement for Microsoft Entra Private Access, Microsoft Entra Internet Access will begin to rollout on October 1, 2024. This is following a 90-day trial period that began with General Availability on July 1st, 2024. Learn more

Basics | Policy Rules | Review

Manage rules in your policy.

+ Add Rule

Name	Destination type	Destination
block komplett.no	Fqdn	*.komplett.no

< Previous | Next >

Authentication methods
Password reset
Custom security attributes
Risky activities
Show more
Identity Governance
Verified ID
Permissions Management
Global Secure Access
Dashboard
Applications
Connect
Traffic forwarding
Client download
Remote networks
Connectors
Secure
Security profiles
Web content filtering policies

Global Secure Access is now in generally available. Licensing requirements have been updated. Licensing enforcement for Microsoft Entra Private Access, Microsoft Entra Internet Access will begin to rollout on with General Availability on July 1st, 2024. Learn more

Basics Policy Rules Review

Review your policy.

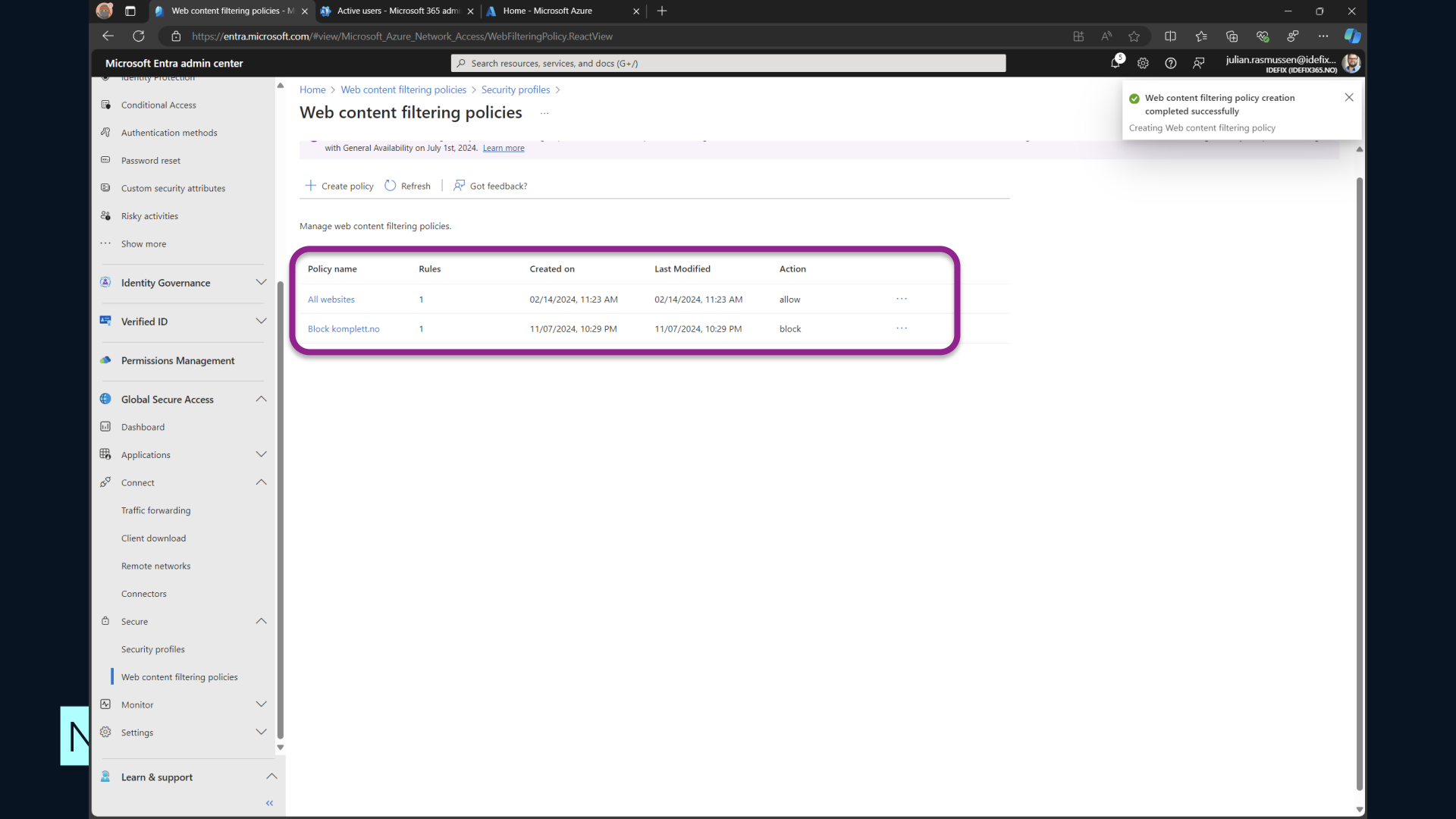
Basics

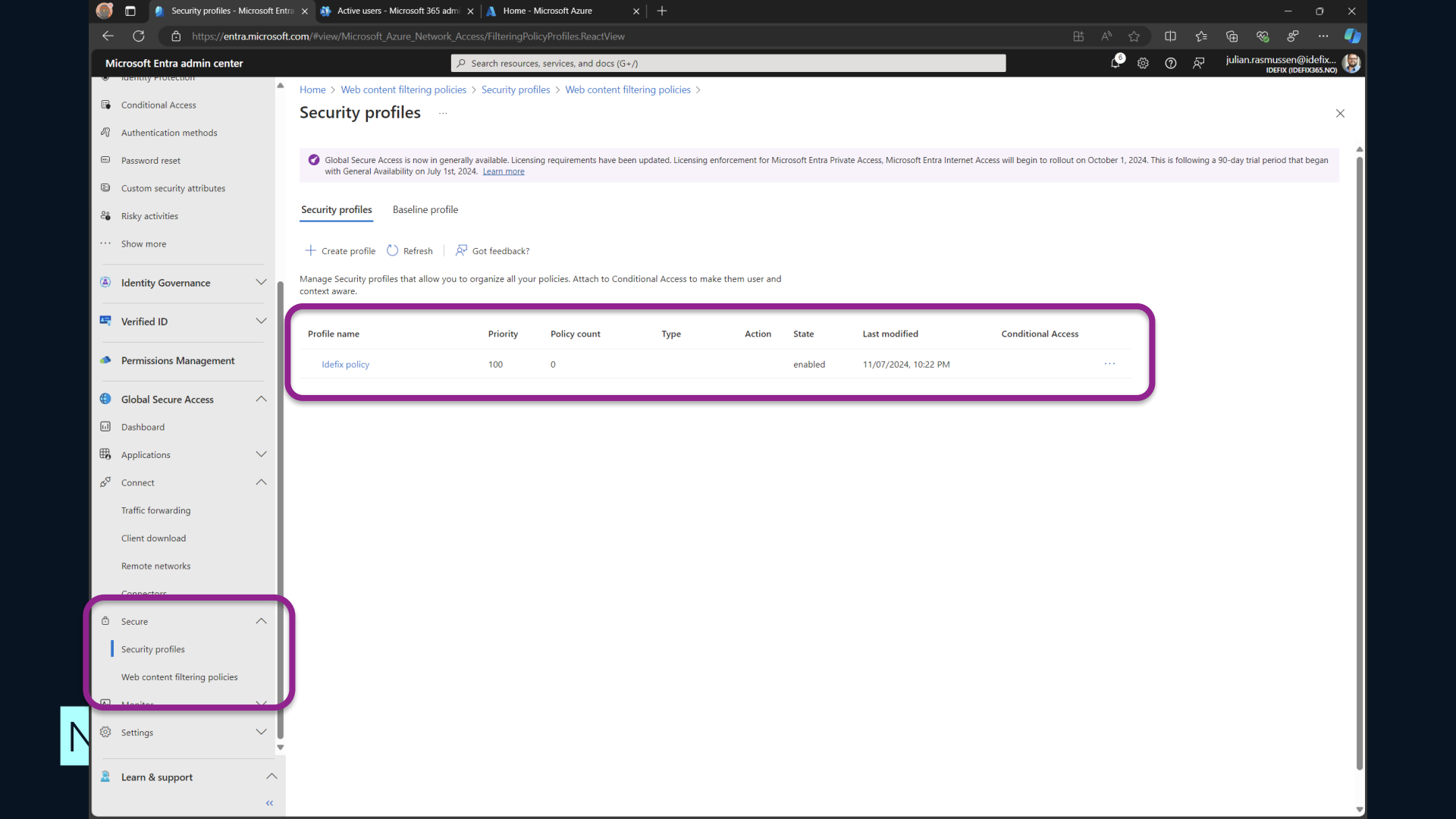
Name	Block komplett.no
Action	block
Description	Content filter for blocking komplett.no websites

Policy Rules

Rules	1

Name	Destination type	Destination
block komplett.no	Fqdn	*.komplett.no


Web content filtering policies - M
Active users - Microsoft 365 admi
Home - Microsoft Azure
https://entra.microsoft.com/#view/Microsoft_Azure_Network_Access/WebFilteringPolicy.ReactView
Microsoft Entra admin center
Search resources, services, and docs (G+/)
julian.rasmussen@idefix...
IDEFIX (IDEFIX365.NO)
Conditional Access
Authentication methods
Password reset
Custom security attributes
Risky activities
Show more
Identity Governance
Verified ID
Permissions Management
Global Secure Access
Dashboard
Applications
Connect
Traffic forwarding
Client download
Remote networks
Connectors
Secure
Security profiles
Web content filtering policies
Monitor
Settings
Learn & support
Home > Web content filtering policies > Security profiles >
Web content filtering policies
with General Availability on July 1st, 2024. Learn more
Web content filtering policy creation completed successfully
Creating Web content filtering policy
Create policy
Refresh
Got feedback?
Manage web content filtering policies.
Policy name
Rules
Created on
Last Modified
Action
All websites
1
02/14/2024, 11:23 AM
02/14/2024, 11:23 AM
allow
Block komplett.no
1
11/07/2024, 10:29 PM
11/07/2024, 10:29 PM
block


Security profiles - Microsoft Entra
Active users - Microsoft 365 admi
Home - Microsoft Azure
https://entra.microsoft.com/#view/Microsoft_Azure_Network_Access/FilteringPolicyProfiles.ReactView
Microsoft Entra admin center
Search resources, services, and docs (G+/)
julian.rasmussen@idefix...
IDEFIX (IDEFIX365.NO)
Conditional Access
Authentication methods
Password reset
Custom security attributes
Risky activities
Show more
Identity Governance
Verified ID
Permissions Management
Global Secure Access
Dashboard
Applications
Connect
Traffic forwarding
Client download
Remote networks
Secure
Security profiles
Web content filtering policies
Settings
Learn & support
Home > Web content filtering policies > Security profiles > Web content filtering policies >
Security profiles
Global Secure Access is now in generally available. Licensing requirements have been updated. Licensing enforcement for Microsoft Entra Private Access, Microsoft Entra Internet Access will begin to rollout on October 1, 2024. This is following a 90-day trial period that began with General Availability on July 1st, 2024. Learn more
Security profiles
Baseline profile
Create profile
Refresh
Got feedback?
Manage Security profiles that allow you to organize all your policies. Attach to Conditional Access to make them user and context aware.
Profile name
Priority
Policy count
Type
Action
State
Last modified
Conditional Access
Idefix policy
100
0
enabled
11/07/2024, 10:22 PM

Create a profile

Global Secure Access is now in generally available. Licensing requirements have been updated. Licensing enforcement for Microsoft Entra Private Access, Microsoft Entra Internet Access will begin to rollout on October 1, 2024. This is following a 90-day trial period that began with General Availability on July 1st, 2024. Learn more

Basics | Link policies | Review

Create a new Security profile for your organization. This user will have a profile name like "Social Media for Marketing", a priority among other policy profiles and a state of "Enabled" or "Disabled".

Profile name * Idefix policy

Description Our security profile for web

State * enabled

Priority * 100

Create a profile

Global Secure Access is now in generally available. Licensing requirements have been updated. Licensing enforcement for Microsoft Entra Private Access, Microsoft Entra Internet Access will begin to rollout on October 1, 2024. This is following a 90-day trial period that began with General Availability on July 1st, 2024. Learn more

Basics | Link policies | Review

Link policies and assign a desired priority to the security profile.

+ Link a policy

- Create new policy
- Existing policy

State	Rules

Identity Protection
Conditional Access
Authentication methods
Password reset
Custom security attributes
Risky activities
Show more
Identity Governance
Verified ID
Permissions Management
Global Secure Access
Dashboard
Applications
Connect
Traffic forwarding
Client download
Remote networks
Connectors
Secure
Security profiles
Web content filtering policies
Monitor
Settings

Create a profile

Global Secure Access is now in generally available. Licensing requirements have been updated. Licensing enforcement for Microsoft Entra Private Access, Microsoft Entra Inte
with General Availability on July 1st, 2024. Learn more

Basics | Link policies | Review

Link policies and assign a desired priority to the security profile.

+ Link a policy

Policy name	Priority	State	Rules

Link a policy

Global Secure Access is now in generally available. Licensing requirements have been updated. Licensing enforcement for Microsoft Entra Private Access, Microsoft Entra Internet Access will begin to rollout on October 1, 2024. This is following a 90-day trial period that began with General Availability on July 1st, 2024. Learn more

Link policies to your profile and assign priority, action, and state values.

Policy name* Block komplett.no

Priority* 100

State* Enabled

Conditional Access
Authentication methods
Password reset
Custom security attributes
Risky activities
Show more
Identity Governance
Verified ID
Permissions Management
Global Secure Access
Dashboard
Applications
Connect
Traffic forwarding
Client download
Remote networks
Connectors
Secure
Security profiles
Web content filtering policies
Monitor
Settings
Learn & support

Create a profile

Global Secure Access is now in generally available. Licensing requirements have been updated. Licensing enforcement for Microsoft Entra Private Access, Microsoft Entra Internet Access will begin to rollout on October 1, 2024. This is following a 90-day trial period that began with General Availability on July 1st, 2024. Learn more

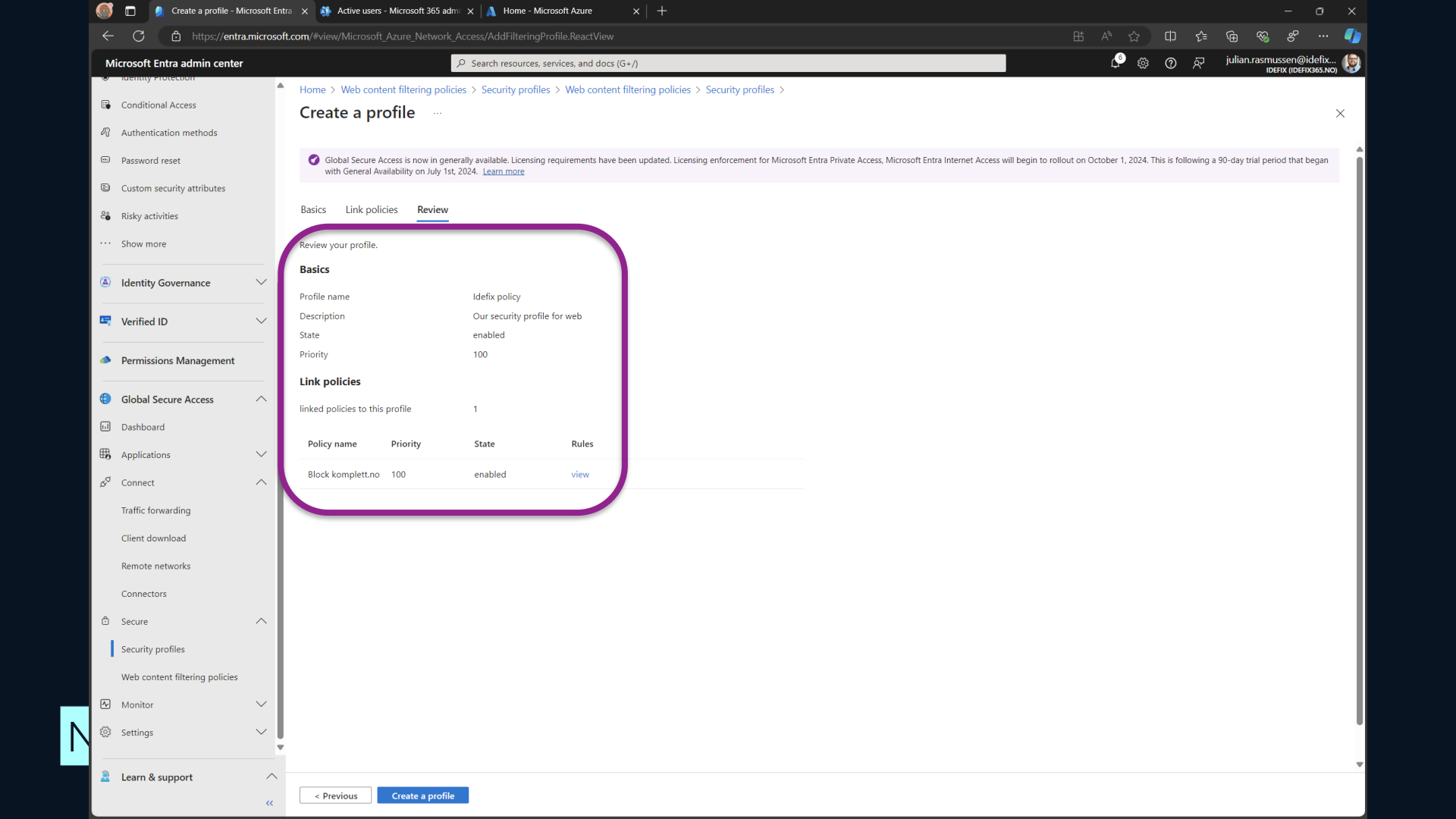
Basics | Link policies | Review

Link policies and assign a desired priority to the security profile.

+ Link a policy

Policy name	Priority	State	Rules
Block komplett.no	100	enabled	view

< Previous | Next >


Create a profile - Microsoft Entra
Active users - Microsoft 365 admi
Home - Microsoft Azure
https://entra.microsoft.com/#view/Microsoft_Azure_Network_Access/AddFilteringProfile.ReactView
Microsoft Entra admin center
Search resources, services, and docs (G+/)
julian.rasmussen@idefix...
IDEFIX (IDEFIX365.NO)
Conditional Access
Authentication methods
Password reset
Custom security attributes
Risky activities
Show more
Identity Governance
Verified ID
Permissions Management
Global Secure Access
Dashboard
Applications
Connect
Traffic forwarding
Client download
Remote networks
Connectors
Secure
Security profiles
Web content filtering policies
Monitor
Settings
Learn & support
Home > Web content filtering policies > Security profiles > Web content filtering policies > Security profiles >
Create a profile
Global Secure Access is now in generally available. Licensing requirements have been updated. Licensing enforcement for Microsoft Entra Private Access, Microsoft Entra Internet Access will begin to rollout on October 1, 2024. This is following a 90-day trial period that began with General Availability on July 1st, 2024. Learn more
Basics
Link policies
Review
Review your profile.
Basics
Profile name
Idefix policy
Description
Our security profile for web
State
enabled
Priority
100
Link policies
linked policies to this profile
1
Policy name
Priority
State
Rules
Block komplett.no
100
enabled
view
< Previous
Create a profile

Identity Protection
Conditional Access
Authentication methods
Password reset
Custom security attributes
Risky activities
Show more
Identity Governance
Verified ID
Permissions Management
Global Secure Access
Dashboard
Applications
Connect
Traffic forwarding
Client download
Remote networks
Connectors
Secure
Security profiles
Web content filtering policies
Monitor
Settings
Learn & support

Conditional Access | Policies

Microsoft Entra ID

Overview
Policies
Insights and reporting
Diagnose and solve problems

Manage
Named locations
Custom controls (Preview)
Terms of use
VPN connectivity
Authentication contexts
Authentication strengths
Classic policies

Monitoring
Sign-in logs
Audit logs

Troubleshooting + Support
New support request

New policy | New policy from template | Upload policy file | What if | Refresh | Preview features | Got feedback?

Microsoft Entra Conditional Access policies are used to apply access controls to keep your organization secure. Learn more

All policies	Microsoft-managed policies
5	0
Total	out of 5

Search | Add filter

5 out of 5 policies found

Policy name	State	Creation date	Modified date
CA001-Global-IdentityProtection-AllApps-AnyPlatform-Grant-MFA	On	6/20/2024, 9:43:39 PM	11/4/2024, 9:49:13 PM
CA002-Global-GSA-AllInternetTraffic-AnyPlatform-Apply-NetworkControl	On	10/29/2024, 9:59:47 AM	11/7/2024, 10:31:05 PM
CA003-Global-GSA-M365Traffic-AnyPlatform-Block-Ex-CompliantNetworkLo...	On	10/31/2024, 10:48:18 PM	11/5/2024, 10:30:10 PM
CA004-Global-GSA-UbuntuSSH-AnyPlatform-Grant-RequireMFA	On	11/7/2024, 12:32:29 PM	11/7/2024, 10:11:19 PM
CA005-Global-GSA-IdefixFiles-AnyPlatform-Grant-RequireMFA	On	11/7/2024, 1:18:02 PM	

ccess | Policies

New policy | New policy from template | Upload policy file | What if | Refresh | Preview features | Got feedback?

Microsoft Entra Conditional Access policies are used to apply access controls to keep your organization secure. Learn more

All policies
5
Total

Microsoft-managed policies
0
out of 5

Search | Add filter

5 out of 5 policies found

Policy name	State	Creation date	Modified date
CA001-Global-IdentityProtection-AllApps-AnyPlatform-Grant-MFA	On	6/20/2024, 9:43:39 PM	11/4/2024, 9:49:13 PM
CA002-Global-GSA-AllInternetTraffic-AnyPlatform-Apply-NetworkControl	On	10/29/2024, 9:59:47 AM	11/7/2024, 10:31:05 PM
CA003-Global-GSA-M365Traffic-AnyPlatform-Block-Ex-CompliantNetworkLo...	On	10/31/2024, 10:48:18 PM	11/5/2024, 10:30:10 PM
CA004-Global-GSA-UbuntuSSH-AnyPlatform-Grant-RequireMFA	On	11/7/2024, 12:32:29 PM	11/7/2024, 10:11:19 PM
CA005-Global-GSA-IdefixFiles-AnyPlatform-Grant-RequireMFA	On	11/7/2024, 1:18:02 PM	

CA002-Global-GSA-AllInternetTraffic-AnyPlatform-Apply-NetworkControl

Conditional Access policy

Delete | View policy information

Control access based on Conditional Access policy to bring signals together, to make decisions, and enforce organizational policies. Learn more

Name *

CA002-Global-GSA-AllInternetTraffic-AnyPla...

Assignments

Users

Specific users included

Target resources

All internet resources with Global Secure Access

Network NEW

Not configured

Conditions

0 conditions selected

Access controls

Grant

1 control selected

Session

Control access based on all or specific apps, internet resources, actions, or authentication context. Learn more

Select what this policy applies to

Resources (formerly cloud apps)

Include | Exclude

- None
- All internet resources with Global Secure Access
- All resources (formerly 'All cloud apps')
- Select resources

To create a Conditional Access policy targeting members in your tenant with Global Secure Access (GSA) as a resource, make sure GSA is deployed in your tenant. Learn more

CA002-Global-GSA-AllInternetTraffic-AnyPlatform-Apply-NetworkControl

Conditional Access policy

Delete | View policy information

Control access based on Conditional Access policy to bring signals together, to make decisions, and enforce organizational policies. Learn more

Name *

CA002-Global-GSA-AllInternetTraffic-AnyPla...

Assignments

Users

Specific users included

Target resources

All internet resources with Global Secure Access

Network NEW

Not configured

Conditions

0 conditions selected

Access controls

Grant

0 controls selected

Session

0 controls selected

Session

Control access based on session controls to enable limited experiences within specific cloud applications. Learn more

- [ ] Use app enforced restrictions

This control only works with supported apps. Currently, Office 365, Exchange Online, and SharePoint Online are the only cloud apps that support app enforced restrictions. Learn more

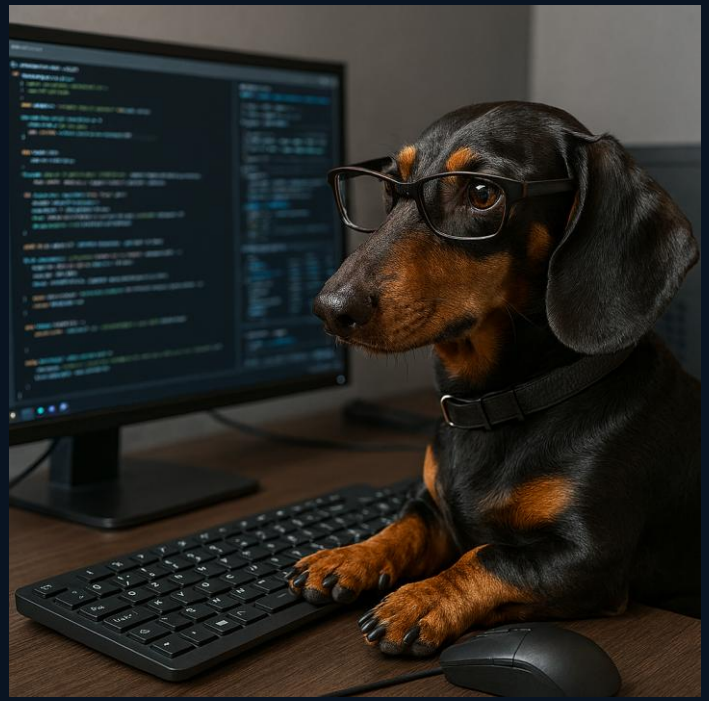
- [ ] Use Conditional Access App Control
- [ ] Sign-in frequency
- [ ] Persistent browser session

Persistent browser session only works correctly when All cloud apps is selected. Please change your cloud apps selection. Learn more

- [ ] Customize continuous access evaluation
- [ ] Disable resilience defaults
- [ ] Require token protection for sign-in sessions (Preview)
- [x] Use Global Secure Access security profile

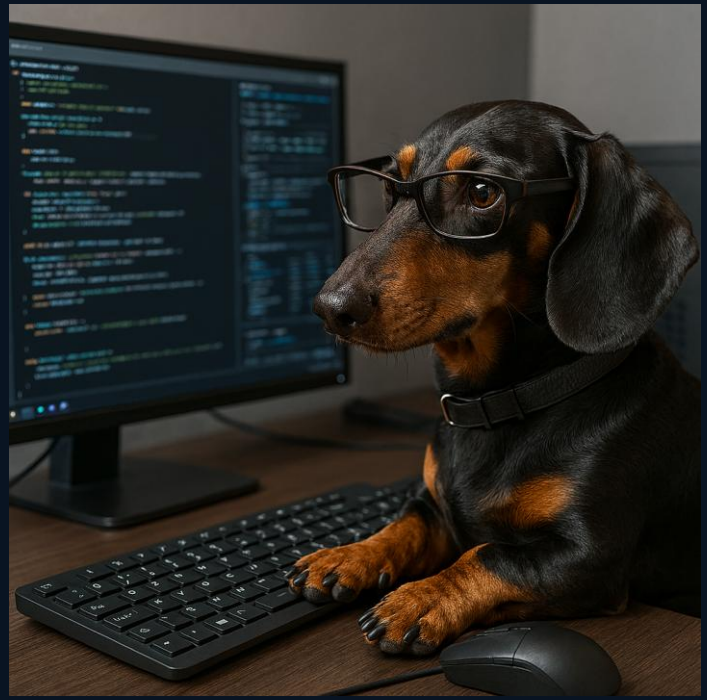
Idefix policy

Browsing komplett.no with GSE client DISABLED



NIC REBEL EDITION

Browsing komplett.no with GSE client ENABLED



NIC REBEL EDITION

What to block

- Adult content
- Gambling & betting
- Known bad sites
- Social media & networking
- Filesharing
- Online games

NIC REBEL EDITION

Client adjustments

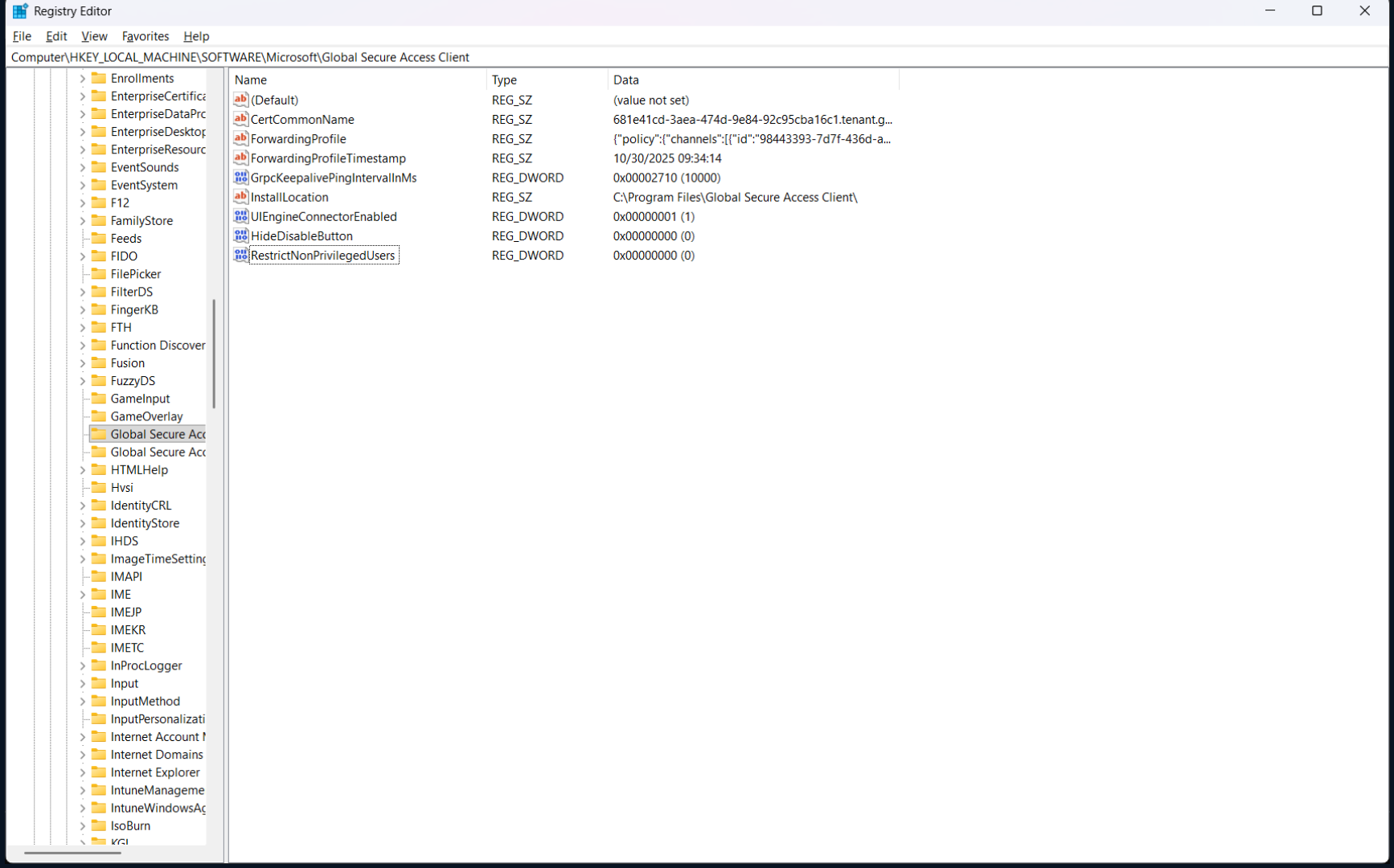
NIC REBEL EDITION

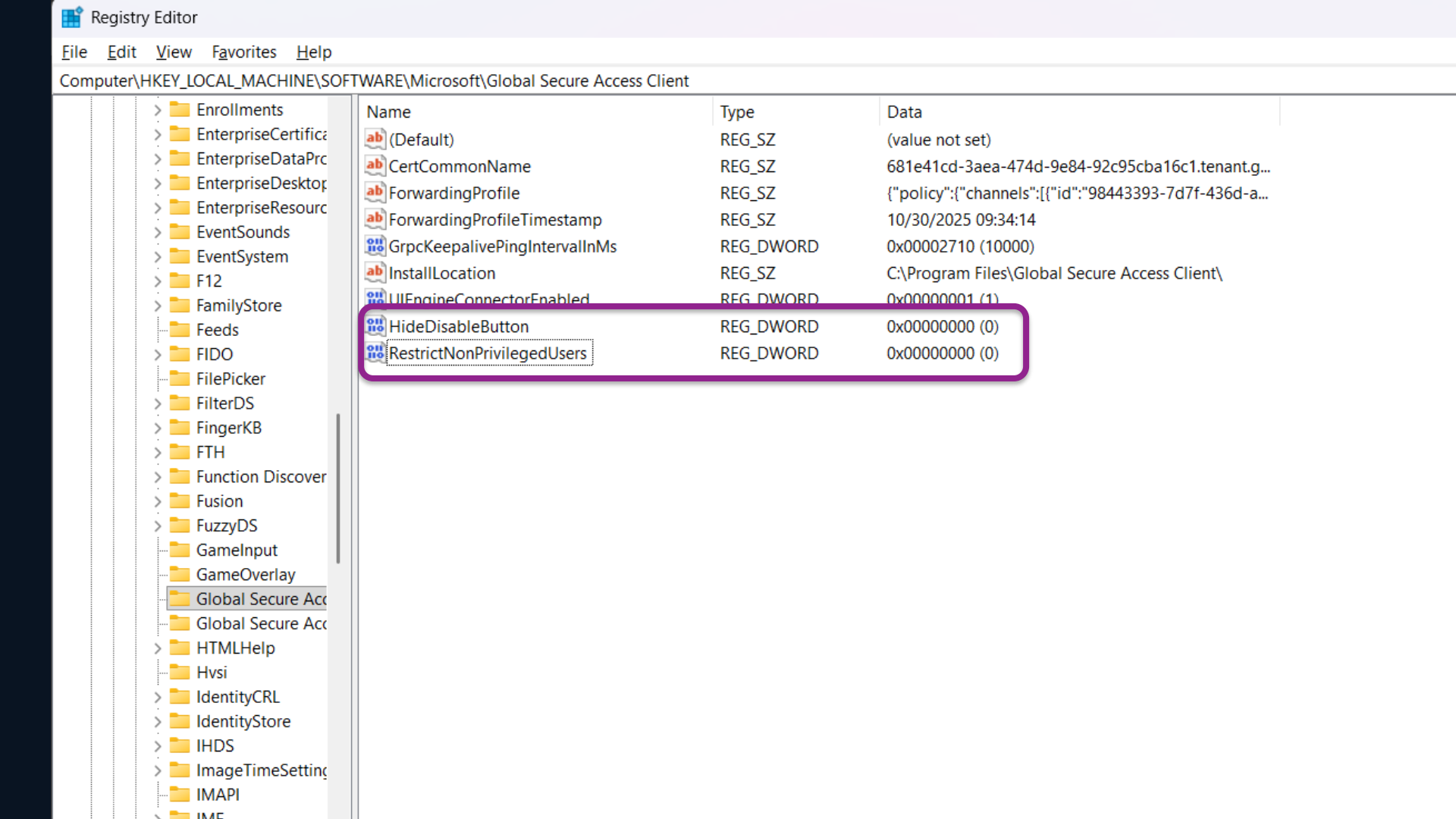
Computer\HKEY_LOCAL_MACHINE\Software\Microsoft\Global Secure Access Client
RestrictNonPrivilegedUsers REG_DWORD

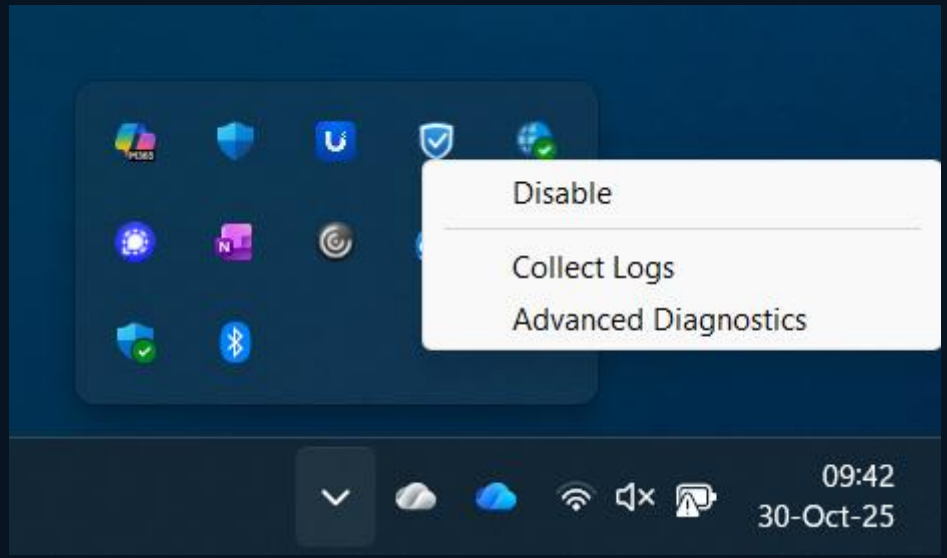
Data	Description
0x0	Nonprivileged users on the Windows device can disable and enable the client.
0x1	Nonprivileged users on the Windows device are restricted from disabling and enabling the client. A UAC prompt requires local administrator credentials for disable and enable options. The administrator can also hide the disable button (see Hide or unhide system tray menu buttons).

NIC REBEL EDITION

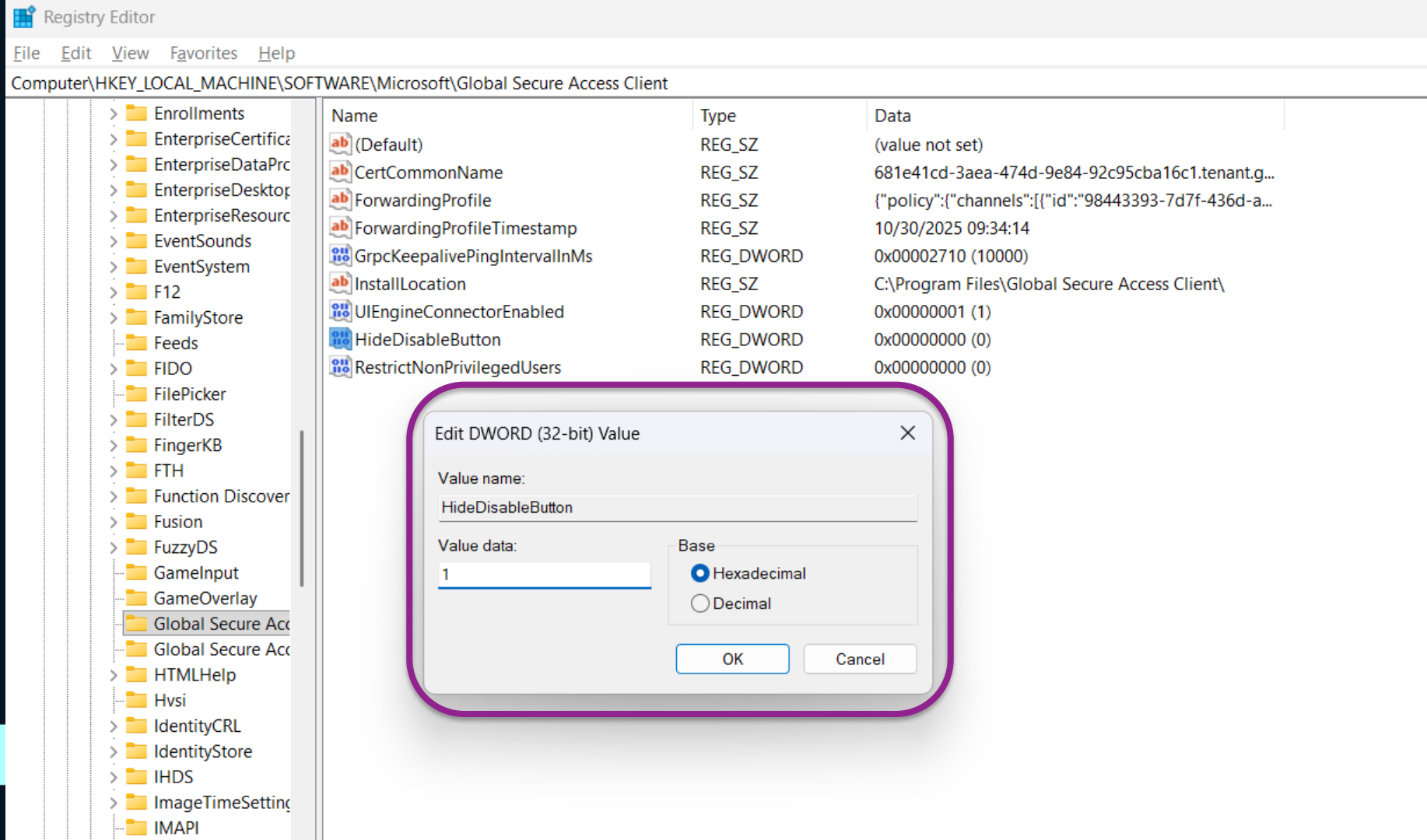
Value	Type	Data	Default behavior	Description
HideSignOutButton	REG_DWORD	0x0 - shown 0x1 - hidden	hidden	Configure this setting to show or hide the **Sign out** action. This option is for specific scenarios when a user needs to sign in to the client with a different Microsoft Entra user than the one used to sign in to Windows. Note: You must sign in to the client with a user in the same Microsoft Entra tenant to which the device is joined. You can also use the **Sign out** action to reauthenticate the existing user.
HideDisablePrivateAccessButton	REG_DWORD	0x0 - shown 0x1 - hidden	hidden	Configure this setting to show or hide the **Disable Private Access** action. This option is for a scenario when the device is directly connected to the corporate network and the user prefers accessing private applications directly through the network instead of through the Global Secure Access.
HideDisableButton	REG_DWORD	0x0 - shown 0x1 - hidden	shown	Configure this setting to show or hide the **Disable** action. When visible, the user can disable the Global Secure Access client. The client remains disabled until the user enables it again. If the **Disable** action is hidden, a nonprivileged user can't disable the client.

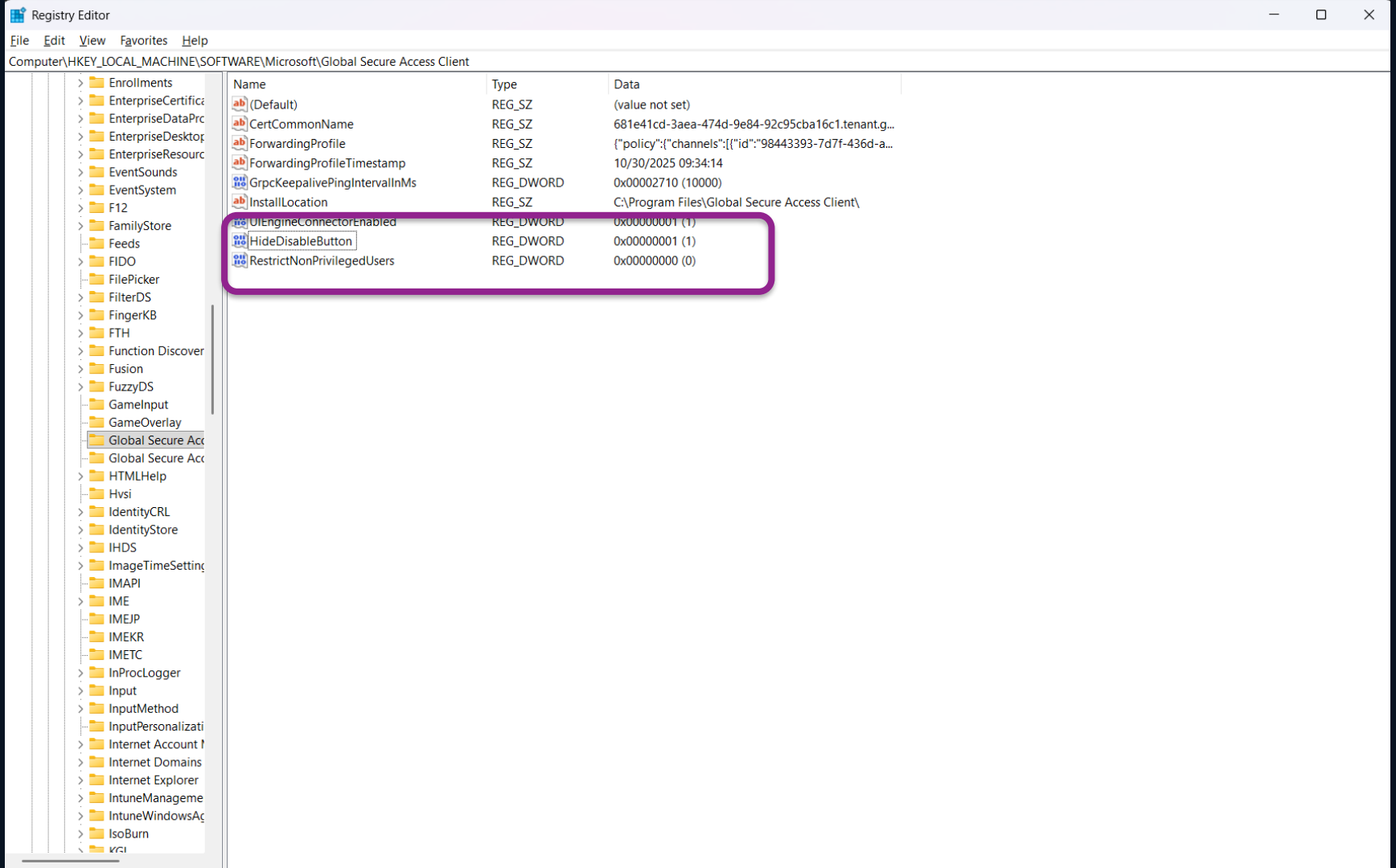

Registry Editor
File Edit View Favorites Help
Computer\HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Global Secure Access Client
Enrollments
EnterpriseCertifica
EnterpriseDataPrc
EnterpriseDesktop
EnterpriseResourc
EventSounds
EventSystem
F12
FamilyStore
Feeds
FIDO
FilePicker
FilterDS
FingerKB
FTH
Function Discover
Fusion
FuzzyDS
GameInput
GameOverlay
Global Secure Acc
Global Secure Acc
HTMLHelp
Hvsi
IdentityCRL
IdentityStore
IHDS
ImageTimeSettinc
IMAPI
IME
IMEJP
IMEKR
IMETC
InProcLogger
Input
InputMethod
InputPersonalizati
Internet Account
Internet Domains
Internet Explorer
IntuneManageme
IntuneWindowsAc
IsoBurn
KGL
Name Type Data
(Default) REG_SZ (value not set)
CertCommonName REG_SZ 681e41cd-3aea-474d-9e84-92c95cba16c1.tenant.g...
ForwardingProfile REG_SZ {"policy":{"channels":[{"id":"98443393-7d7f-436d-a...
ForwardingProfileTimestamp REG_SZ 10/30/2025 09:34:14
GrpcKeepalivePingIntervalInMs REG_DWORD 0x00002710 (10000)
InstallLocation REG_SZ C:\Program Files\Global Secure Access Client\
UIEngineConnectorEnabled REG_DWORD 0x00000001 (1)
HideDisableButton REG_DWORD 0x00000000 (0)
RestrictNonPrivilegedUsers REG_DWORD 0x00000000 (0)

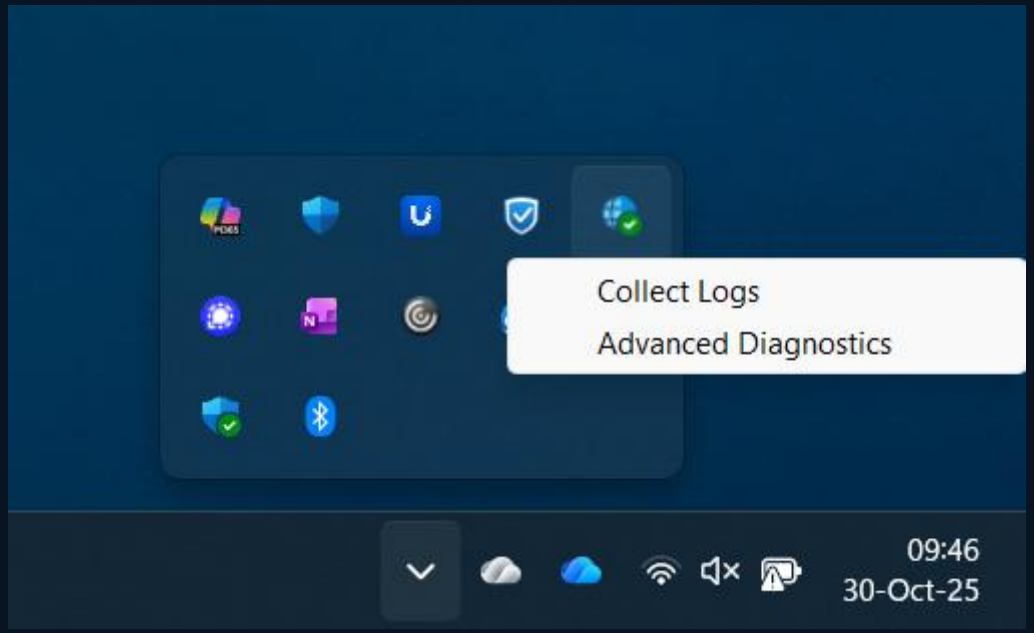

Registry Editor
File Edit View Favorites Help
Computer\HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Global Secure Access Client
EnrollIments
EnterpriseCertifica
EnterpriseDataPrc
EnterpriseDesktop
EnterpriseResourc
EventSounds
EventSystem
F12
FamilyStore
Feeds
FIDO
FilePicker
FilterDS
FingerKB
FTH
Function Discover
Fusion
FuzzyDS
GameInput
GameOverlay
Global Secure Acc
Global Secure Acc
HTMLHelp
Hvsi
IdentityCRL
IdentityStore
IHDS
ImageTimeSettinc
IMAPI
Name
Type
Data
(Default)
REG_SZ
(value not set)
CertCommonName
REG_SZ
681e41cd-3aea-474d-9e84-92c95cba16c1.tenant.g...
ForwardingProfile
REG_SZ
{"policy":{"channels":[{"id":"98443393-7d7f-436d-a...
ForwardingProfileTimestamp
REG_SZ
10/30/2025 09:34:14
GrpcKeepalivePingIntervalInMs
REG_DWORD
0x00002710 (10000)
InstallLocation
REG_SZ
C:\Program Files\Global Secure Access Client\
UIEngineConnectorEnabled
REG_DWORD
0x00000001 (1)
HideDisableButton
REG_DWORD
0x00000000 (0)
RestrictNonPrivilegedUsers
REG_DWORD
0x00000000 (0)



NIC REBEL EDITION


Registry Editor
File Edit View Favorites Help
Computer\HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Global Secure Access Client
Enrollments
EnterpriseCertifica
EnterpriseDataPrc
EnterpriseDesktop
EnterpriseResourc
EventSounds
EventSystem
F12
FamilyStore
Feeds
FIDO
FilePicker
FilterDS
FingerKB
FTH
Function Discover
Fusion
FuzzyDS
GameInput
GameOverlay
Global Secure Acc
Global Secure Acc
HTMLHelp
Hvsi
IdentityCRL
IdentityStore
IHDS
ImageTimeSettinc
IMAPI
Name
Type
Data
(Default)
REG_SZ
(value not set)
CertCommonName
REG_SZ
681e41cd-3aea-474d-9e84-92c95cba16c1.tenant.g...
ForwardingProfile
REG_SZ
{"policy":{"channels":[{"id":"98443393-7d7f-436d-a...
ForwardingProfileTimestamp
REG_SZ
10/30/2025 09:34:14
GrpcKeepalivePingIntervalInMs
REG_DWORD
0x00002710 (10000)
InstallLocation
REG_SZ
C:\Program Files\Global Secure Access Client\
UIEngineConnectorEnabled
REG_DWORD
0x00000001 (1)
HideDisableButton
REG_DWORD
0x00000000 (0)
RestrictNonPrivilegedUsers
REG_DWORD
0x00000000 (0)
Edit DWORD (32-bit) Value
Value name:
HideDisableButton
Value data:
1
Base
Hexadecimal
Decimal
OK
Cancel


Registry Editor
File Edit View Favorites Help
Computer\HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Global Secure Access Client
Enrollments
EnterpriseCertifica
EnterpriseDataPrc
EnterpriseDesktop
EnterpriseResourc
EventSounds
EventSystem
F12
FamilyStore
Feeds
FIDO
FilePicker
FilterDS
FingerKB
FTH
Function Discover
Fusion
FuzzyDS
GameInput
GameOverlay
Global Secure Acc
Global Secure Acc
HTMLHelp
Hvsi
IdentityCRL
IdentityStore
IHDS
ImageTimeSetting
IMAPI
IME
IMEJP
IMEKR
IMETC
InProcLogger
Input
InputMethod
InputPersonalizati
Internet Account
Internet Domains
Internet Explorer
IntuneManageme
IntuneWindowsAg
IsoBurn
Name
Type
Data
(Default)
REG_SZ
(value not set)
CertCommonName
REG_SZ
681e41cd-3aea-474d-9e84-92c95cba16c1.tenant.g...
ForwardingProfile
REG_SZ
{"policy":{"channels":[{"id":"98443393-7d7f-436d-a...
ForwardingProfileTimestamp
REG_SZ
10/30/2025 09:34:14
GrpcKeepalivePingIntervalInMs
REG_DWORD
0x00002710 (10000)
InstallLocation
REG_SZ
C:\Program Files\Global Secure Access Client\
UiEngineConnectorEnabled
REG_DWORD
0x00000001 (1)
HideDisableButton
REG_DWORD
0x00000001 (1)
RestrictNonPrivilegedUsers
REG_DWORD
0x00000000 (0)



NIC REBEL EDITION

Entra ID Private access

NIC REBEL EDITION

Microsoft Entra Private Access

- Enforce Conditional Access across all private resources
- Deliver seamless access to private apps and resources with single sign-on
- Securing just-in-time access to sensitive resources

NIC REBEL EDITION

Microsoft Entra Private Access

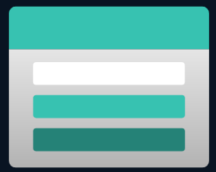
- Secure access to Azure managed service
- Simplify Microsoft Entra private network connector deployment for your private workloads
- Enable edge accelerated Zero Trust private domain name resolution

NIC REBEL EDITION

NIC REBEL EDITION

10.0.0.0/24

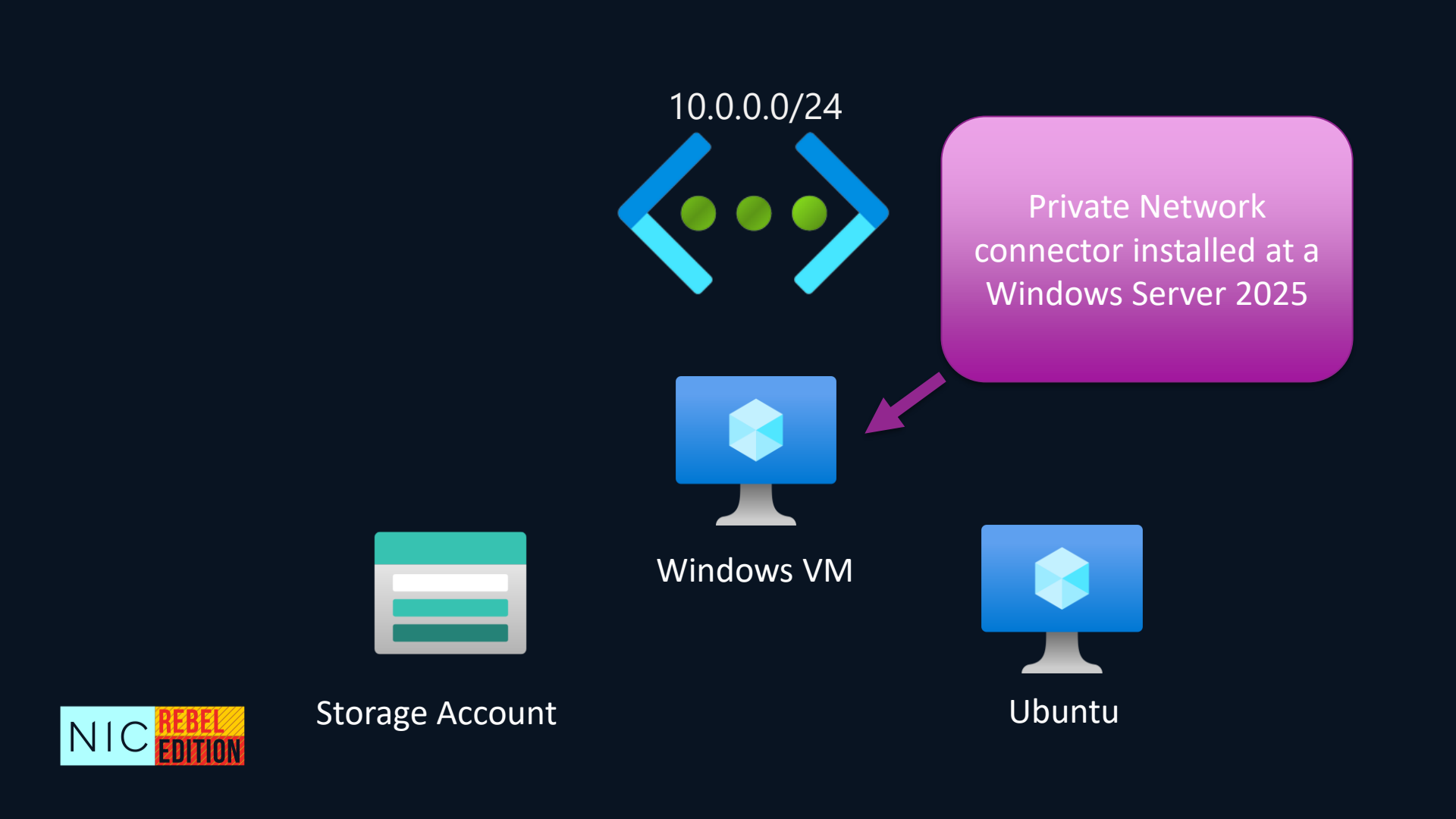
Windows VM

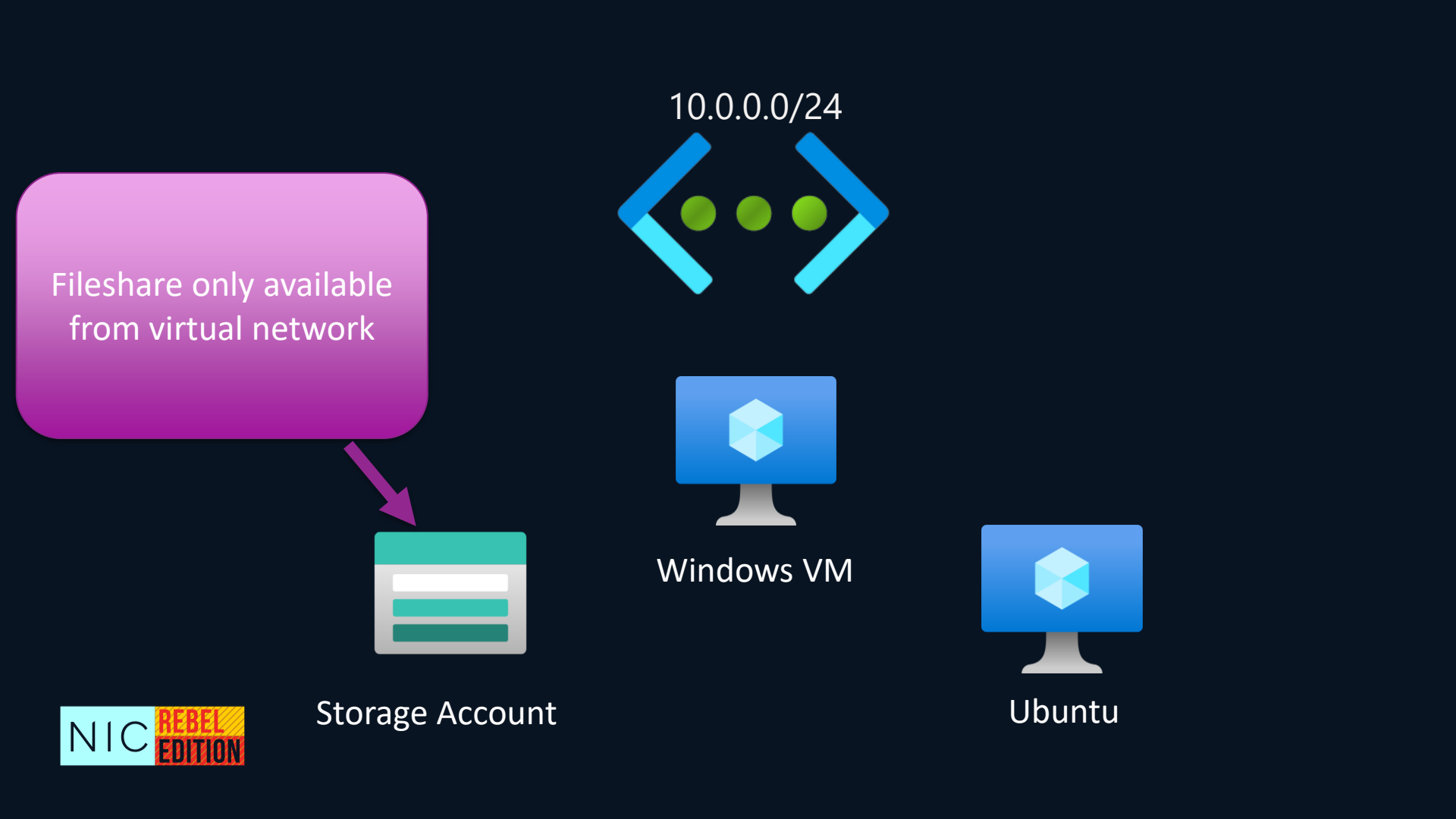


Storage Account

Ubuntu

NIC REBEL EDITION

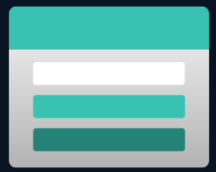

10.0.0.0/24
Private Network connector installed at a Windows Server 2025
Windows VM
Storage Account
Ubuntu
NIC REBEL EDITION


10.0.0.0/24
Fileshare only available from virtual network
Windows VM
Storage Account
Ubuntu
NIC REBEL EDITION

10.0.0.0/24

Ubuntu 24.10 – SSH only allowed from virtual network

Windows VM



Storage Account

Ubuntu

NIC REBEL EDITION

Demo of setup for Private Access

NIC REBEL EDITION

Traffic forwarding

Global Secure Access is now in generally available. Licensing requirements have been updated. Licensing enforcement for Microsoft Entra Private Access, Microsoft Entra Internet Access will begin to rollout on October 1, 2024. This is following a 90-day trial period that began with General Availability on July 1st, 2024. Learn more

Refresh | Got feedback?

Manage traffic forwarding profiles

Traffic forwarding profiles enable admins to forward specific traffic to Global Secure Access. Assign traffic forwarding profiles to users running the Global Secure Access client. For clientless devices, use the Microsoft profile to assign to remote networks.
Learn more

One or more profiles are configured and ready to use. To finish setup, Download Global Secure Access client.

Microsoft traffic profile

Enabled
Last modified on 10/31/2024, 10:59 PM

Applies to
Internet traffic to Microsoft services

Microsoft traffic policies
3 policies View

Linked Conditional Access policies
2 policies View

User and group assignments
1 users, 0 groups assigned View

Remote network assignments
0 assigned remote networks View

Private access profile

Enabled
Last modified on 11/07/2024, 01:16 PM

Applies to
Private resources

Private access policies
Quick Access, 2 Applications View

Linked Conditional Access policies
None

User and group assignments
2 users, 0 groups assigned View

Remote network assignments
Not applicable

Internet access profile

Enabled
Last modified on not available

Applies to
All internet traffic, except for the Microsoft traffic profile

Internet access policies
3 policies View

Linked Conditional Access policies
2 policies View

User and group assignments
2 users, 0 groups assigned View

Remote network assignments
Not applicable

Protection
Identity Protection
Conditional Access
Authentication methods
Password reset
Custom security attributes
Risky activities
Show more
Identity Governance
Verified ID
Permissions Management
Global Secure Access
Dashboard
Connect
Traffic forwarding
Client download
Remote networks
Connectors
Secure
Monitor
Settings
Learn & support

Private Network connectors

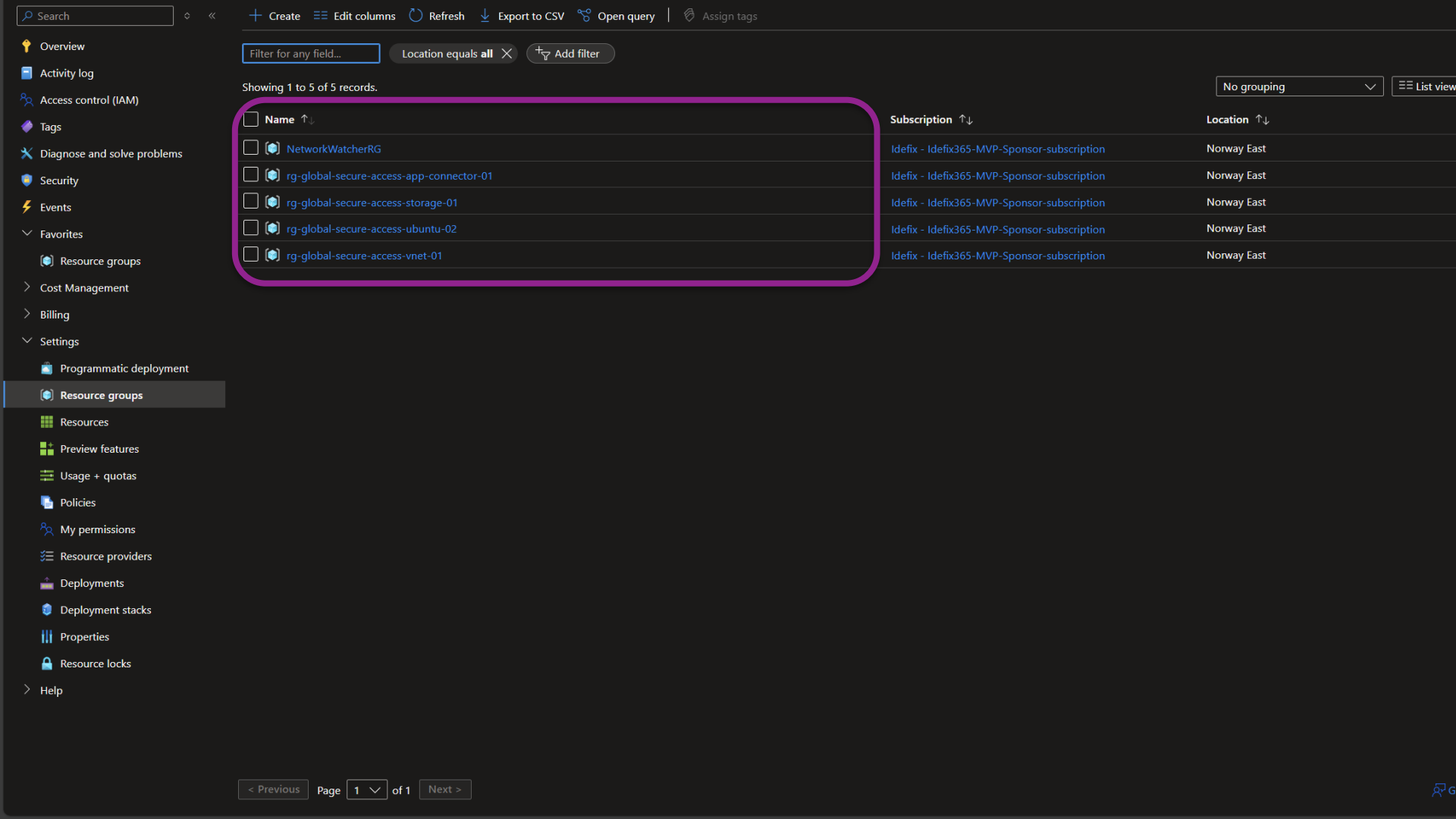
New Connector Group | Download connector service | Configure an app | Disable Private Network connectors | Got feedback?

Microsoft Entra Private Network provides single sign-on (SSO) and secure remote access for web applications hosted on-premises.
Learn more about Microsoft Entra Private Network connectors

Connectors

Connectors establish a secure communication channel between your on-premises network and Azure.

H...	Groups	IP	Status	Country/Region
	Default			Europe
	vm-windows-01	51.120.1.197	Active	


Search
Create
Edit columns
Refresh
Export to CSV
Open query
Assign tags
Overview
Activity log
Access control (IAM)
Tags
Diagnose and solve problems
Security
Events
Favorites
Resource groups
Cost Management
Billing
Settings
Programmatic deployment
Resource groups
Resources
Preview features
Usage + quotas
Policies
My permissions
Resource providers
Deployments
Deployment stacks
Properties
Resource locks
Help
Filter for any field...
Location equals all
Add filter
Showing 1 to 5 of 5 records.
No grouping
List view
Name
Subscription
Location
NetworkWatcherRG
rg-global-secure-access-app-connector-01
rg-global-secure-access-storage-01
rg-global-secure-access-ubuntu-02
rg-global-secure-access-vnet-01
Idefix - Idefix365-MVP-Sponsor-subscription
Norway East
< Previous
Page 1 of 1
Next >

Firewalls and virtual networks | Private endpoint connections | Custom domain

Save | Discard | Refresh | Give feedback

Public network access

- ○ Enabled from all networks
- ◉ Enabled from selected virtual networks and IP addresses
- ○ Disabled

Configure network security for your storage accounts. Learn more

Virtual networks

+ Add existing virtual network + Add new virtual network

Virtual Network	Subnet	Address range	Endpoint Status	Resource Group	Subscript
vnet-servers-01	1			rg-global-secure-access-vnet-01	Idefix - Id
	default	10.0.0.0/24	✓ Enabled	rg-global-secure-access-vnet-01	Idefix - Id

Firewall

Add IP ranges to allow access from the internet or your on-premises networks. Learn more.

☐ Add your client IP address ('80.232.2.138')

Address range
213.239.102.46
IP address or CIDR

Resource instances

Specify resource instances that will have access to your storage account based on their system-assigned managed identity.

Resource type	Instance name
Select a resource type	Select one or more instances

Exceptions

Protection
Identity Protection
Conditional Access
Authentication methods
Password reset
Custom security attributes
Risky activities
Show more
Identity Governance
Verified ID
Permissions Management
Global Secure Access
Dashboard
Applications
Quick Access
Application discovery
Enterprise applications
Connect
Traffic forwarding
Client download
Remote networks
Connectors

Enterprise applications

New application | Refresh | Download (Export) | Preview info | Columns | Preview features | Got feedback?

View, filter, and search applications in your organization that are set up to use your Microsoft Entra tenant as their Identity Provider.

The list of applications that are maintained by your organization are in application registrations.

Search by application name or object ID | Application type == **Global Secure Access applications** | Application ID starts with | Add filters

2 applications found

Name	Object ID	Application ID
IF Idefix files	10b8ce1c-6e4f-4e42-8bd1-b04dcf9db88c	7964647f-c89c-42fe-989e-04d3f361eabb
US Ubuntu SSH	77f05e2f-9dc3-41a8-b283-6c7571159810	604aad8d-66dd-4c2e-9acc-9a23f34b23f8

Active users - Microsoft 365 admi | idefixfilestorage01 - Microsoft Az

com/#view/Microsoft_AAD_IAM/NetworkAccessApplication.ReactView/appId//objectId//fromNav/globalSecureAccess

Search resources, services, and docs (G+/)

julian.rasmussen@idefix...
IDEFIX (IDEFIX365.NO)

Home > Enterprise applications >

Create Global Secure Access application

Got feedback?

Global Secure Access is now generally available. Licensing requirements have been updated. Learn more

Name * SQL Access

Connector Group Default

We recommend at least two active connectors in selected group 'Default'. Click here to download a connector or manage your connector groups.

Enable access with Global Secure Access client

Application Segment

Add application segment

Destination type	Destination	Ports	Protocol	Status	Delete

Create application segment

Destination type: IP address

IP address *: 10.0.0.9

Ports *: 1433

Protocol *: TCP

Status: Pending

Custom security attributes
Risky activities
Show less
Identity Governance
Verified ID
Permissions Management
Global Secure Access
Dashboard
Applications
Quick Access
Application discovery
Enterprise applications
Connect
Traffic forwarding
Client download
Remote networks
Connectors
Secure
Security profiles
Web content filtering policies
Monitor
Alerts

Quick Access | Create Quick Access configuration

Manage
Create Quick Access configuration

Edit application settings | Got feedback?

Global Secure Access is now generally available. Licensing requirements have been updated. Learn more

Name * SQL Access

Connector Group Default

We recommend at least two active connectors in selected group 'Default'. Click here to download a connector or manage your connector groups.

Application Segment | Private DNS PREVIEW

+ Add Quick Access application segment

Destination type	Destination	Ports	Protocol	Status	Delete
Fully qualified domain n...	http://test	1433	TCP	Pending	

Custom security attributes
Risky activities
Show less
Identity Governance
Verified ID
Permissions Management
Global Secure Access
Dashboard
Applications
Quick Access
Application discovery
Enterprise applications
Connect
Traffic forwarding
Client download
Remote networks
Connectors
Secure
Security profiles
Web content filtering policies
Monitor
Alerts

Quick Access | Create Quick Access configuration

Manage
Create Quick Access configuration

Edit application settings | Got feedback?

Global Secure Access is now generally available. Licensing requirements have been updated. Learn more

Name * SQL Access

Connector Group Default

We recommend at least two active connectors in selected group 'Default'. Click here to download a connector or manage your connector groups.

Application Segment | Private DNS PREVIEW

Enable Private DNS

Add DNS Suffix(s) to use for private DNS.Learn more

Add DNS suffix

DNS suffix
idefix.no

Overview
Policies
Insights and reporting
Diagnose and solve problems

Manage
Named locations
Custom controls (Preview)
Terms of use
VPN connectivity
Authentication contexts
Authentication strengths
Classic policies

Monitoring
Sign-in logs
Audit logs

Troubleshooting + Support
New support request

Microsoft Entra Conditional Access policies are used to apply access controls to keep your organization secure. Learn more

All policies	Microsoft-managed policies
5	0
Total	out of 5

Search | Add filter

5 out of 5 policies found

Policy name	State	Creation date	Modified date
CA001-Global-IdentityProtection-AllApps-AnyPlatform-Grant-MFA	On	6/20/2024, 9:43:39 PM	11/4/2024, 9:49:13 PM
CA002-Global-GSA-AllInternetTraffic-AnyPlatform-Apply-NetworkControl	On	10/29/2024, 9:59:47 AM	11/7/2024, 10:38:33 PM
CA003-Global-GSA-M365Traffic-AnyPlatform-Block-Ex-CompliantNetworkLo...	On	10/31/2024, 10:48:18 PM	11/5/2024, 10:30:10 PM
CA004-Global-GSA-UbuntuSSH-AnyPlatform-Grant-RequireMFA-EveryTime	On	11/7/2024, 12:32:29 PM	11/7/2024, 11:07:26 PM
CA005-Global-GSA-IdefixFiles-AnyPlatform-Grant-RequireMFA	On	11/7/2024, 1:18:02 PM	

Control access based on Conditional Access policy to bring signals together, to make decisions, and enforce organizational policies. Learn more

Name *

CA004-Global-GSA-UbuntuSSH-AnyPlatfor...

Assignments

Users

Specific users included

Target resources

1 resource included

Not configured

Conditions

0 conditions selected

Access controls

Grant

1 control selected

Session

Sign-in frequency - Every time

Control access based on all or specific apps, internet resources, actions, or authentication context. Learn more

Select what this policy applies to

Resources (formerly cloud apps)

Include Exclude

- None
- All internet resources with Global Secure Access
- All resources (formerly 'All cloud apps')
- Select resources

Edit filter

None

Select

Ubuntu SSH

Ubuntu SSH
604aad8d-66dd-4c2e-9acc-9a23f34b23f8

Over prompting users for reauthentication can occur when the "Sign-in Frequency - every time" setting is enabled in some applications. Read more about the recommended scenarios.

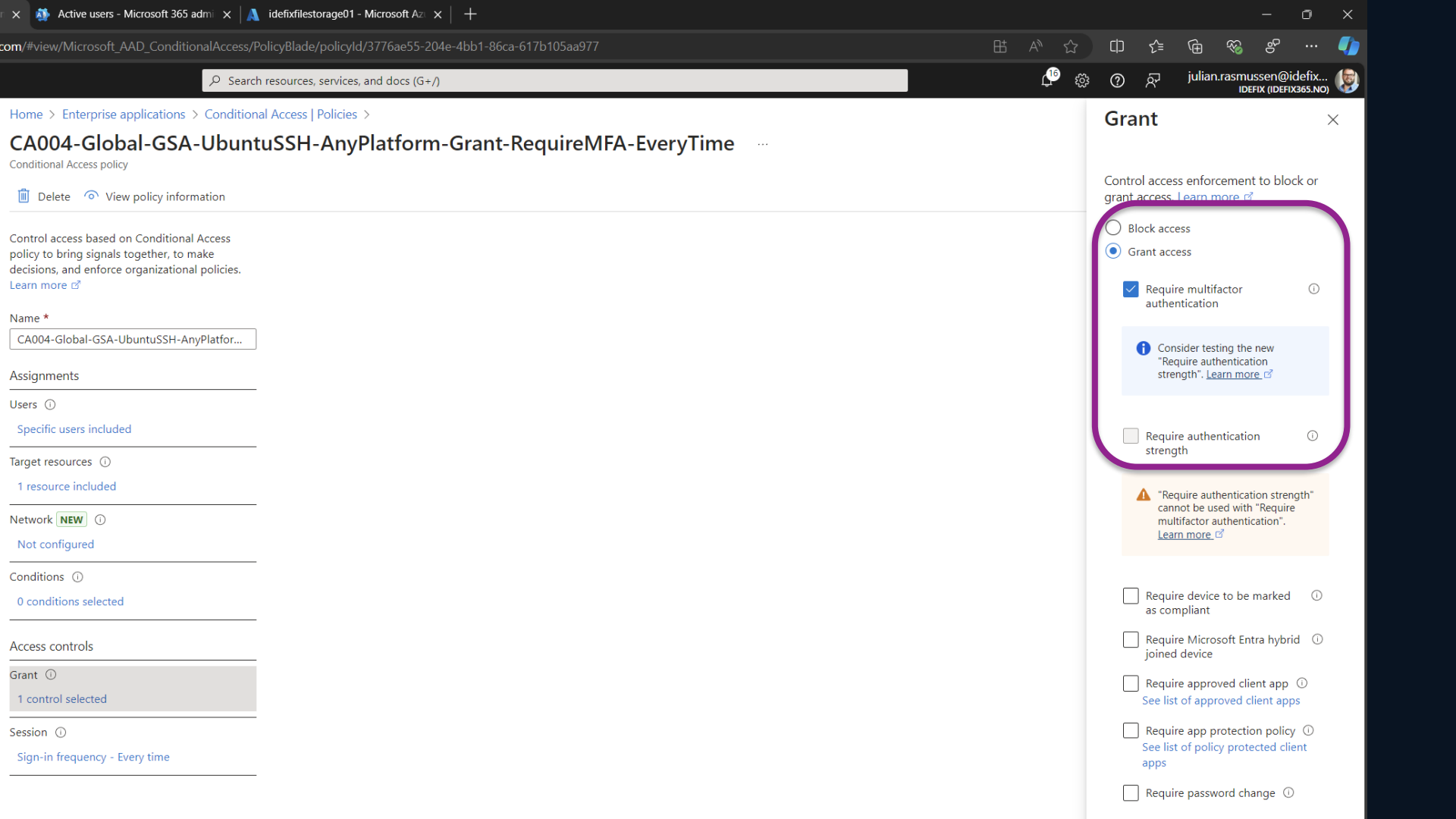
To create a Conditional Access policy targeting members in your tenant with Global Secure Access (GSA) as a resource, make sure GSA is deployed in

Over prompting users for reauthentication can occur when the "Sign-in Frequency - every time" setting is enabled in some applications. Read more about the recommended scenarios.

Enable policy

Report-only On Off

Save


Active users - Microsoft 365 admi
idefixfilestorage01 - Microsoft Az
com/#view/Microsoft_AAD_ConditionalAccess/PolicyBlade/policyId/3776ae55-204e-4bb1-86ca-617b105aa977
Search resources, services, and docs (G+/)
julian.rasmussen@idefix...
IDEFIX (IDEFIX365.NO)
Home > Enterprise applications > Conditional Access | Policies >
CA004-Global-GSA-UbuntuSSH-AnyPlatform-Grant-RequireMFA-EveryTime
Conditional Access policy
Delete
View policy information
Control access based on Conditional Access policy to bring signals together, to make decisions, and enforce organizational policies.
Learn more
Name *
CA004-Global-GSA-UbuntuSSH-AnyPlatfor...
Assignments
Users
Specific users included
Target resources
1 resource included
Network NEW
Not configured
Conditions
0 conditions selected
Access controls
Grant
1 control selected
Session
Sign-in frequency - Every time
Grant
Control access enforcement to block or grant access. Learn more
Block access
Grant access
Require multifactor authentication
Consider testing the new "Require authentication strength". Learn more
Require authentication strength
"Require authentication strength" cannot be used with "Require multifactor authentication". Learn more
Require device to be marked as compliant
Require Microsoft Entra hybrid joined device
Require approved client app
See list of approved client apps
Require app protection policy
See list of policy protected client apps
Require password change

Control access based on Conditional Access policy to bring signals together, to make decisions, and enforce organizational policies.
Learn more

Name *
CA004-Global-GSA-UbuntuSSH-AnyPlatfor...

Assignments

Users
Specific users included

Target resources
1 resource included

Network NEW
Not configured

Conditions
0 conditions selected

Access controls

Grant
1 control selected

Session
Sign-in frequency - Every time

Over prompting users for reauthentication can occur when the "Sign-in Frequency - every time" setting is enabled in some applications. Read more about the recommended scenarios.

Enable policy
Report-only | On | Off

Save

Use app enforced restrictions

This control only works with supported apps. Currently, Office 365, Exchange Online, and SharePoint Online are the only cloud apps that support app enforced restrictions. Learn more

Use Conditional Access App Control

Sign-in frequency
- Periodic reauthentication
- Every time

Persistent browser session

Customize continuous access evaluation

Disable resilience defaults

Require token protection for sign-in sessions (Preview)

Use Global Secure Access security profile

This option only works with Global Secure Access resources.

Select

DEMO SSH

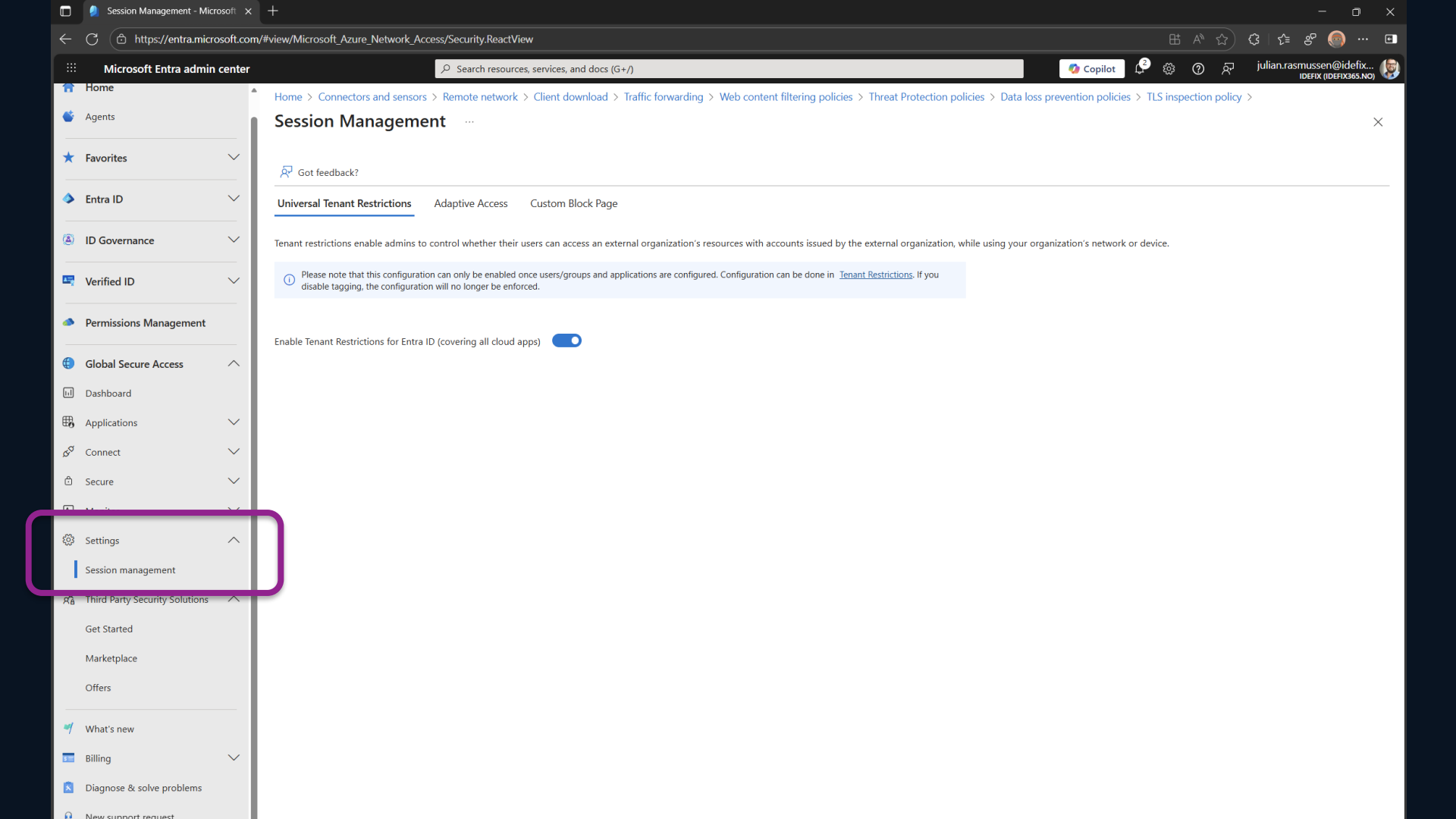
NIC REBEL EDITION

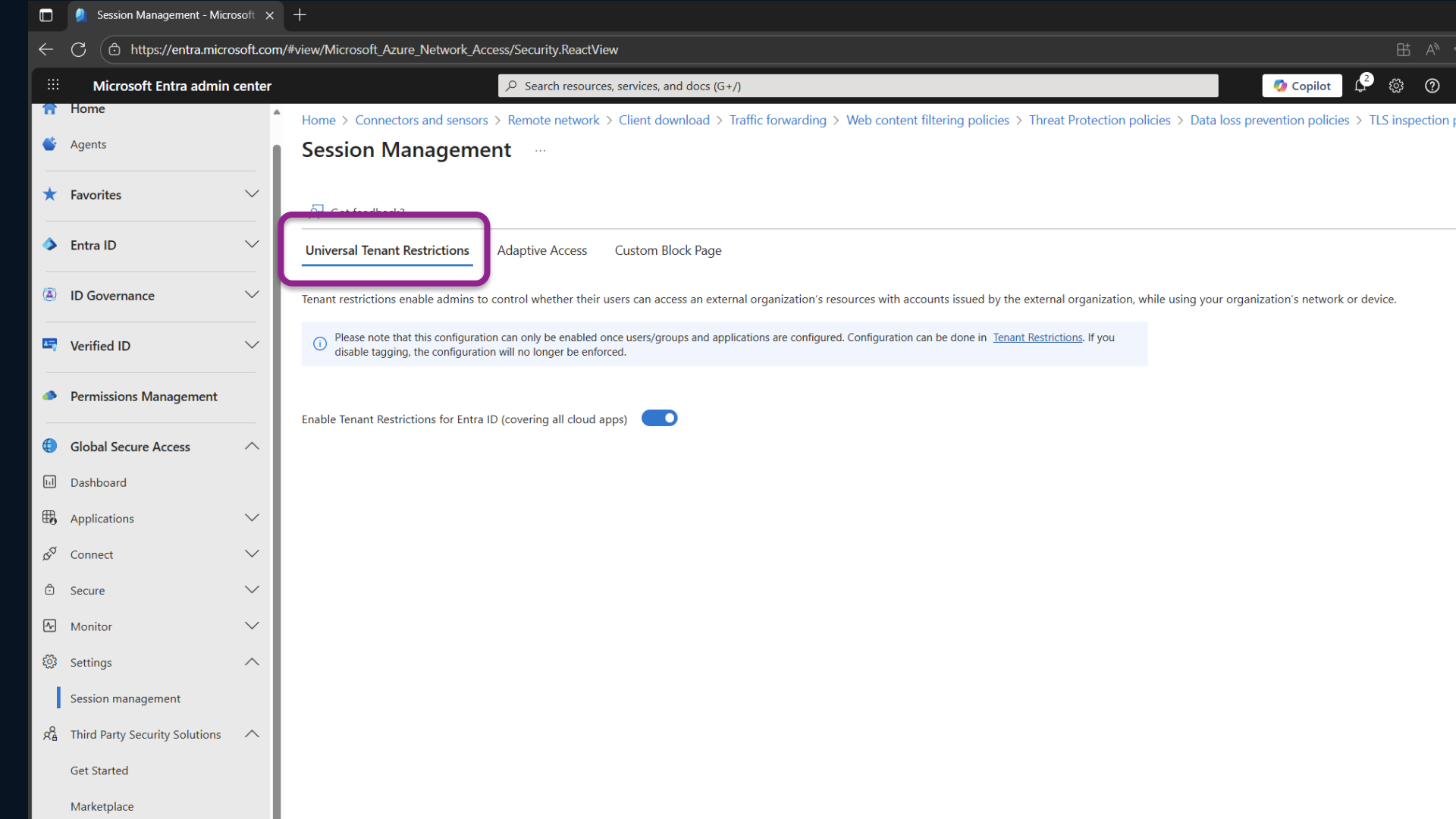
DEMO Storage Account

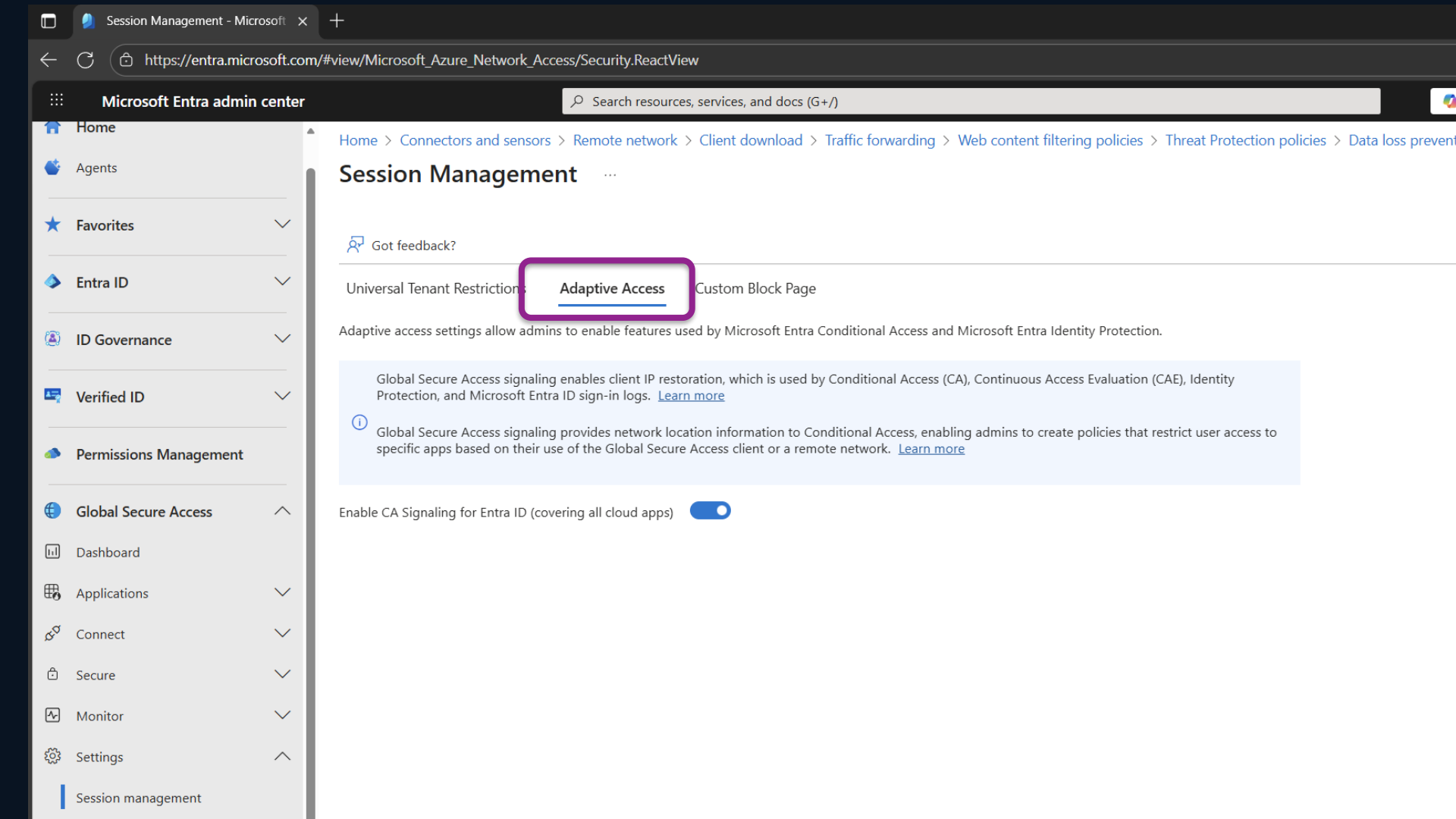
NIC REBEL EDITION

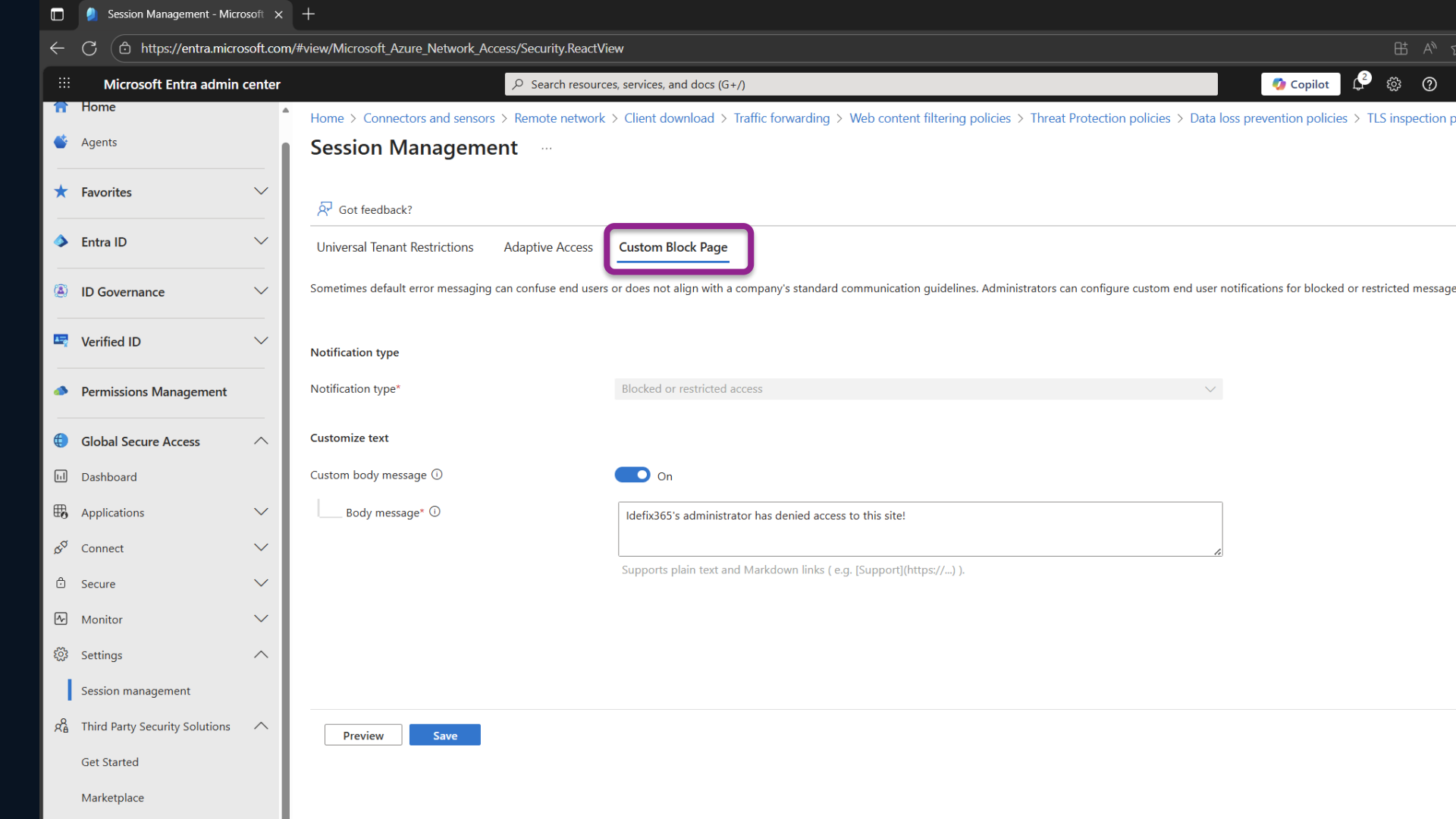
Settings

NIC REBEL EDITION


Session Management - Microsoft
https://entra.microsoft.com/#view/Microsoft_Azure_Network_Access/Security.ReactView
Microsoft Entra admin center
Search resources, services, and docs (G+/)
Copilot
julian.rasmussen@idefix...
IDEFIX (IDEFIX365.NO)
Home
Agents
Favorites
Entra ID
ID Governance
Verified ID
Permissions Management
Global Secure Access
Dashboard
Applications
Connect
Secure
Settings
Session management
Third Party Security Solutions
Get Started
Marketplace
Offers
What's new
Billing
Diagnose & solve problems
Home > Connectors and sensors > Remote network > Client download > Traffic forwarding > Web content filtering policies > Threat Protection policies > Data loss prevention policies > TLS inspection policy >
Session Management
Got feedback?
Universal Tenant Restrictions
Adaptive Access
Custom Block Page
Tenant restrictions enable admins to control whether their users can access an external organization's resources with accounts issued by the external organization, while using your organization's network or device.
Please note that this configuration can only be enabled once users/groups and applications are configured. Configuration can be done in Tenant Restrictions. If you disable tagging, the configuration will no longer be enforced.
Enable Tenant Restrictions for Entra ID (covering all cloud apps)


Session Management - Microsoft
https://entra.microsoft.com/#view/Microsoft_Azure_Network_Access/Security.ReactView
Microsoft Entra admin center
Search resources, services, and docs (G+/)
Copilot
Home
Agents
Favorites
Entra ID
ID Governance
Verified ID
Permissions Management
Global Secure Access
Dashboard
Applications
Connect
Secure
Monitor
Settings
Session management
Third Party Security Solutions
Get Started
Marketplace
Home > Connectors and sensors > Remote network > Client download > Traffic forwarding > Web content filtering policies > Threat Protection policies > Data loss prevention policies > TLS inspection
Session Management
Universal Tenant Restrictions
Adaptive Access
Custom Block Page
Tenant restrictions enable admins to control whether their users can access an external organization's resources with accounts issued by the external organization, while using your organization's network or device.
Please note that this configuration can only be enabled once users/groups and applications are configured. Configuration can be done in Tenant Restrictions. If you disable tagging, the configuration will no longer be enforced.
Enable Tenant Restrictions for Entra ID (covering all cloud apps)


Session Management - Microsoft
https://entra.microsoft.com/#view/Microsoft_Azure_Network_Access/Security.ReactView
Microsoft Entra admin center
Search resources, services, and docs (G+/)
Home
Agents
Favorites
Entra ID
ID Governance
Verified ID
Permissions Management
Global Secure Access
Dashboard
Applications
Connect
Secure
Monitor
Settings
Session management
Home > Connectors and sensors > Remote network > Client download > Traffic forwarding > Web content filtering policies > Threat Protection policies > Data loss prevent
Session Management
Got feedback?
Universal Tenant Restrictions
Adaptive Access
Custom Block Page
Adaptive access settings allow admins to enable features used by Microsoft Entra Conditional Access and Microsoft Entra Identity Protection.
Global Secure Access signaling enables client IP restoration, which is used by Conditional Access (CA), Continuous Access Evaluation (CAE), Identity Protection, and Microsoft Entra ID sign-in logs. Learn more
Global Secure Access signaling provides network location information to Conditional Access, enabling admins to create policies that restrict user access to specific apps based on their use of the Global Secure Access client or a remote network. Learn more
Enable CA Signaling for Entra ID (covering all cloud apps)


Session Management - Microsoft
https://entra.microsoft.com/#view/Microsoft_Azure_Network_Access/Security.ReactView
Microsoft Entra admin center
Search resources, services, and docs (G+/)
Copilot
Home
Agents
Favorites
Entra ID
ID Governance
Verified ID
Permissions Management
Global Secure Access
Dashboard
Applications
Connect
Secure
Monitor
Settings
Session management
Third Party Security Solutions
Get Started
Marketplace
Home > Connectors and sensors > Remote network > Client download > Traffic forwarding > Web content filtering policies > Threat Protection policies > Data loss prevention policies > TLS inspection p
Session Management
Got feedback?
Universal Tenant Restrictions
Adaptive Access
Custom Block Page
Sometimes default error messaging can confuse end users or does not align with a company's standard communication guidelines. Administrators can configure custom end user notifications for blocked or restricted message
Notification type
Notification type*
Blocked or restricted access
Customize text
Custom body message
On
Body message*
Idefix365's administrator has denied access to this site!
Supports plain text and Markdown links (e.g. [Support](https://...)).
Preview
Save

Monitoring

NIC REBEL EDITION

Privileged Identity Management
All users
Identity
Protection
Identity Governance
Verified ID
Permissions Management
Global Secure Access
Dashboard
Applications
Connect
Secure
Monitor
Alerts
Audit logs
Traffic logs
Deployment logs
Remote network health logs
Enriched Microsoft 365 logs
Workbooks
Settings
Learn & support

Home > Gallery >

Idefix

Global Secure Access is now in generally available. Licensing requirements have been updated. Licensing enforcement for Microsoft Entra Private Access, Microsoft Entra Internet Access will begin to rollout on October 1, 2024. This is following a 90-day trial period that began with General Availability on July 1st, 2024. Learn more

Welcome to Global Secure Access

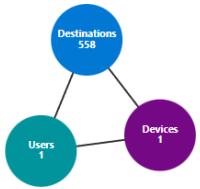
Secure access and improve visibility to the internet, Microsoft 365, SaaS, and private apps. Learn more about Global Secure Access

Get Started with the dashboard | Got feedback?

Last 24 hours

Global Secure Access snapshot

Traffic type : All



The Global Secure Access snapshots provides quick access to the users, devices, and destinations with network traffic captured by Microsoft Entra Private Access and Microsoft Entra Internet Access.

Out of 10 devices, 1 have the Global Secure Access Client installed: 10.0%

Device status

Active devices

1 ▲ 0% in the last 24 hours

The number of distinct active devices that signed in to other tenants in the last 24 hours

Alerts and notifications PREVIEW

1 notifications in the last 24 hours

Alert name	
15 sites categorized as SocialNetworking were blocked	Check the traffic logs

Top used destinations

Review the top-used destinations by traffic type.

All | Microsoft 365 | Internet Access | Private Access

Sort by : Transactions

westeurope-shared.prod.warm.ingest.monitor.core.windows.net	9.6K

Idefix

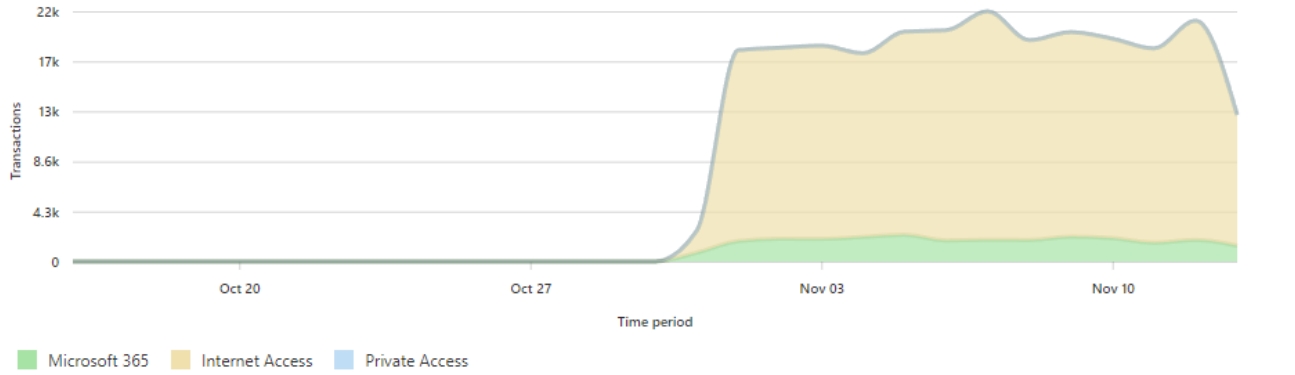
Alerts and notifications PREVIEW

1 notifications in the last 24 hours

Alert name	
15 sites categorized as SocialNetworking were blocked	Check the traffic logs

Usage profiling PREVIEW

Display by : Transactions Date : Last month



Top used destinations

Review the top-used destinations by traffic type.

All Microsoft 365 Internet Access

Sort by : Transactions

westeurope-shared.prod.warm.ingest.monitor.core.
login.microsoftonline.com
gcs.prod.monitoring.core.windows.net
advmetric-black.prod.microsoftmetrics.com
advmetric-red.prod.microsoftmetrics.com

Idefix

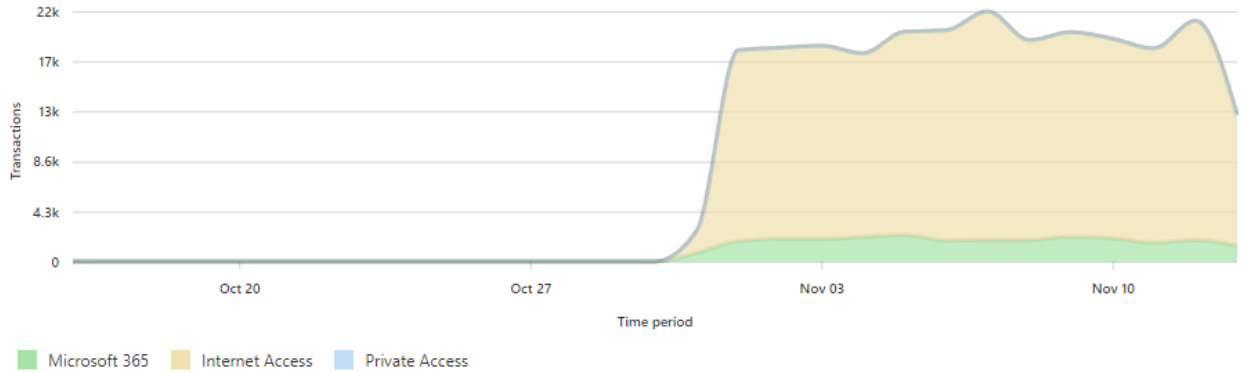
Alerts and notifications PREVIEW

1 notifications in the last 24 hours

Alert name	
15 sites categorized as SocialNetworking were blocked	Check the traffic logs

Usage profiling PREVIEW

Display by : Transactions Date : Last month



Top used destinations

Review the top-used destinations by traffic type.

All Microsoft 365 Internet Access

Sort by : Transactions

westeurope-shared.prod.warm.ingest.monitor.core.
login.microsoftonline.com
gcs.prod.monitoring.core.windows.net
advmetric-black.prod.microsoftmetrics.com
advmetric-red.prod.microsoftmetrics.com

Idefix ...

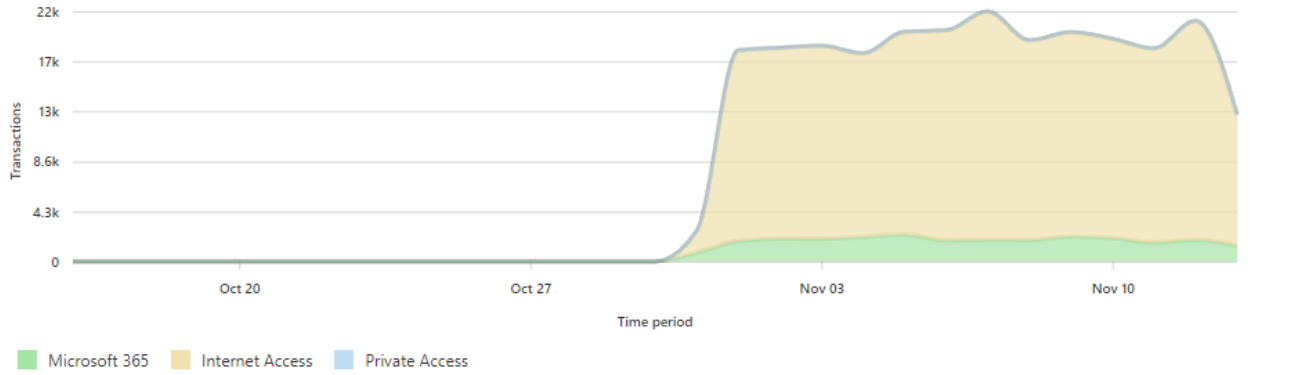
Alerts and notifications PREVIEW

1 notifications in the last 24 hours

Alert name	
15 sites categorized as SocialNetworking were blocked	Check the traffic logs

Usage profiling PREVIEW

Display by : Transactions Date : Last month



Top used destinations

Review the top-used destinations by traffic type.

All Microsoft 365 Internet Access

Sort by : Transactions

westeurope-shared.prod.warm.ingest.monitor.core.
login.microsoftonline.com
gcs.prod.monitoring.core.windows.net
advmetric-black.prod.microsoftmetrics.com
advmetric-red.prod.microsoftmetrics.com

Idefix

View details

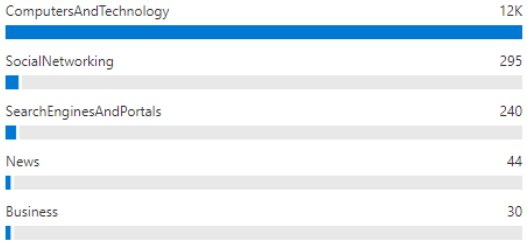
View all destinations

Web category filtering

Review destination web categories accessed by your users. Access to specific categories can be blocked using Conditional Access and web filtering policy.

All | Blocked | Allowed

Sort by : Transactions



View all web categories

Cross-tenant access

Tenant accessed by your users may increase the risk of data loss.

Total sessions
20

Total distinct tenants	1
Rarely used tenants	1
Users	1
Devices	1

Configure tenant restrictions | View details

Device status

Inactive devices
1 ▲ 0% in the last 24 hours

The number of inactive devices that signed in to other tenants in the last 24 hours

View details

View all destinations

Web category filtering

Review destination web categories accessed by your users. Access to specific categories can be blocked using Conditional Access and web filtering policy.

All | Blocked | Allowed

Sort by : Transactions

SocialNetworking 295

View all web categories

Cross-tenant access

Tenant accessed by your users may increase the risk of data loss.

Total sessions
20

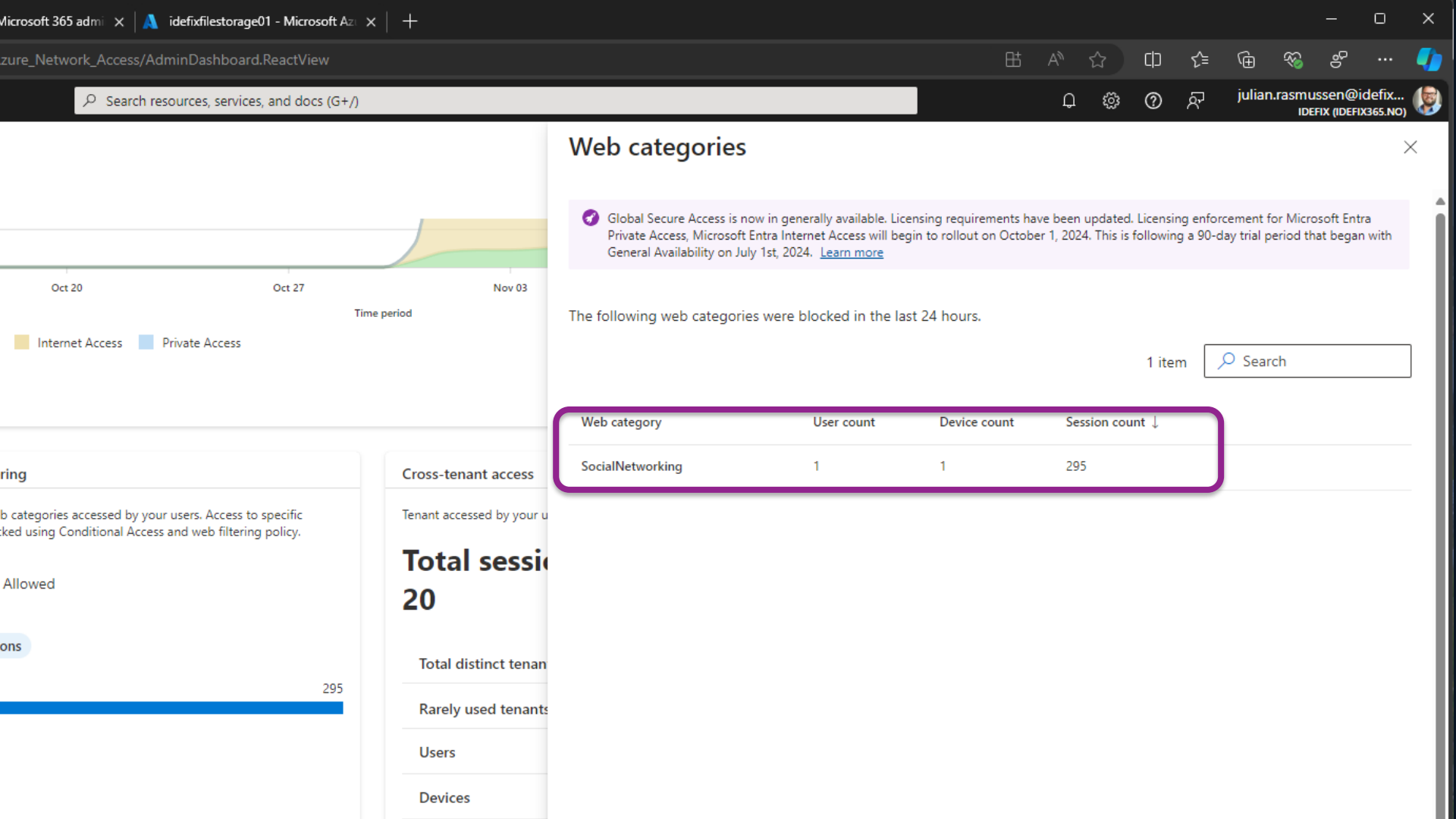
Total distinct tenants	1
Rarely used tenants	1
Users	1
Devices	1

Configure tenant restrictions | View details

Device status

Inactive devices
1 ▲ 0% in the last 24 hours

The number of inactive devices that signed in to other tenants in the last 24 hours


Microsoft 365 admi
idefixfilestorage01 - Microsoft Az
zure_Network_Access/AdminDashboard.ReactView
Search resources, services, and docs (G+/)
julian.rasmussen@idefix...
IDEFIX (IDEFIX365.NO)
Oct 20
Oct 27
Nov 03
Time period
Internet Access
Private Access
ring
b categories accessed by your users. Access to specific
cked using Conditional Access and web filtering policy.
Allowed
ons
295
Cross-tenant access
Tenant accessed by your u
Total sessi
20
Total distinct tenan
Rarely used tenants
Users
Devices
Web categories
Global Secure Access is now in generally available. Licensing requirements have been updated. Licensing enforcement for Microsoft Entra Private Access, Microsoft Entra Internet Access will begin to rollout on October 1, 2024. This is following a 90-day trial period that began with General Availability on July 1st, 2024. Learn more
The following web categories were blocked in the last 24 hours.
1 item
Search
Web category
User count
Device count
Session count
SocialNetworking
1
1
295

View details

View all destinations

Web category filtering

Review destination web categories accessed by your users. Access to specific categories can be blocked using Conditional Access and web filtering policy.

All | Blocked | Allowed

Sort by : Transactions

SocialNetworking 29

View all web categories

Cross-tenant access

Tenant accessed by your users may increase the risk of data loss.

Total sessions
20

Total distinct tenants	1
Rarely used tenants	1
Users	1
Devices	1

Configure tenant restrictions | View details

Device status

Inactive devices
1 ▲ 0% in the last 24 hours

The number of inactive devices that signed in to other tenants in the last 24 hours

Idefix

View details

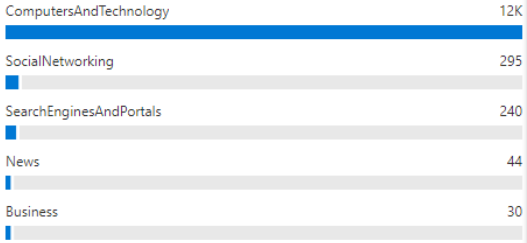
View all destinations

Web category filtering

Review destination web categories accessed by your users. Access to specific categories can be blocked using Conditional Access and web filtering policy.

All | Blocked | Allowed

Sort by : Transactions



View all web categories

Cross-tenant access

Tenant accessed by your users may increase the risk of data loss.

Total sessions
20

Total distinct tenants	1
Rarely used tenants	1
Users	1
Devices	1

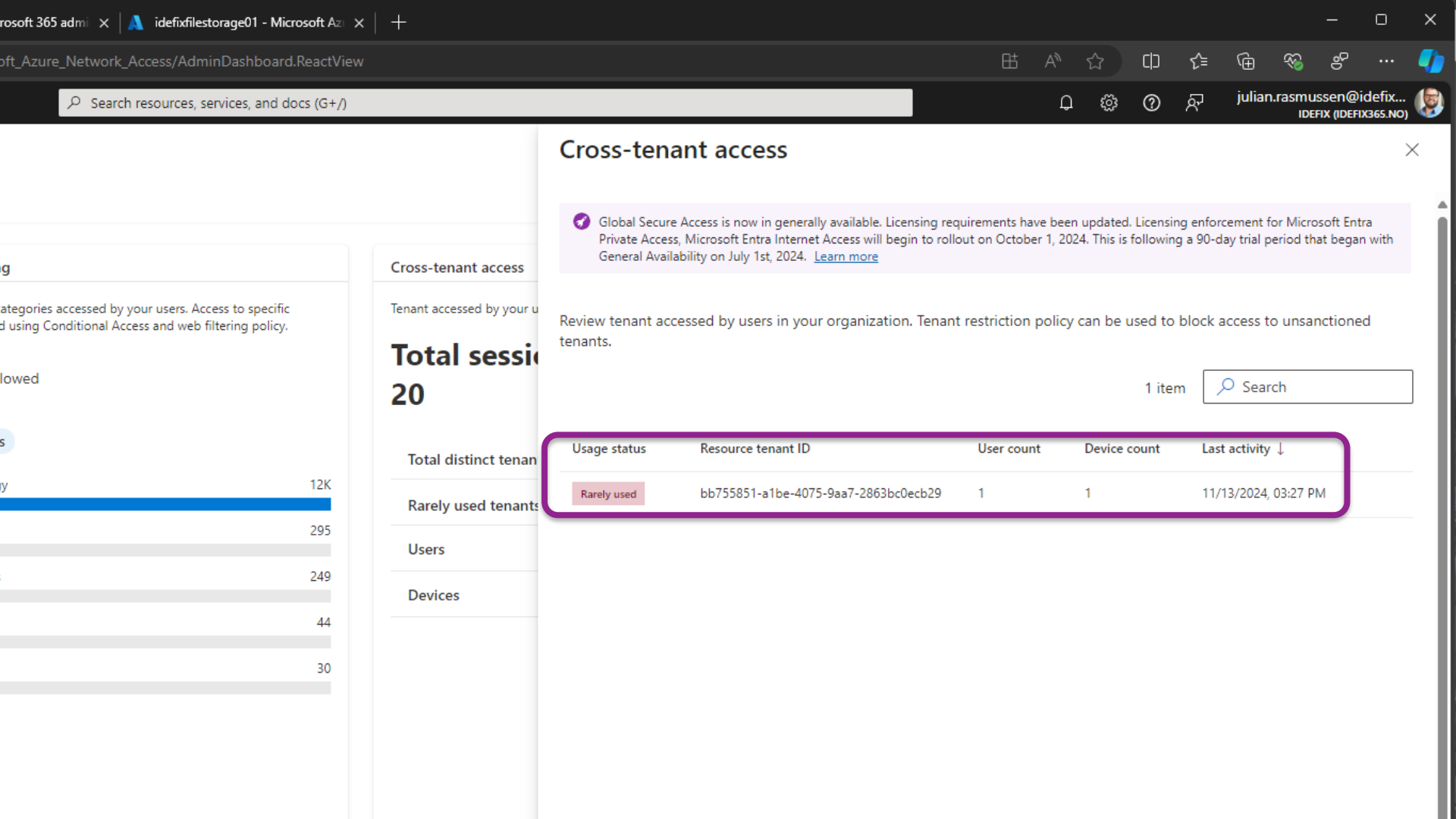
Configure tenant restrictions | View details

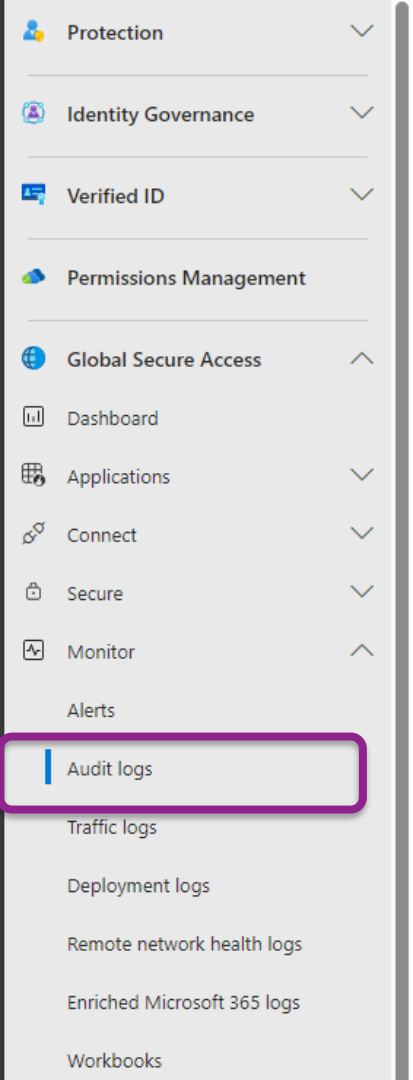
Device status

Inactive devices

1 ▲ 0% in the last 24 hours

The number of inactive devices that signed in to other tenants in the last 24 hours


idefixfilestorage01 - Microsoft Az
oft_Azure_Network_Access/AdminDashboard.ReactView
Search resources, services, and docs (G+/)
julian.rasmussen@idefix...
IDEFIX (IDEFIX365.NO)
Cross-tenant access
Global Secure Access is now in generally available. Licensing requirements have been updated. Licensing enforcement for Microsoft Entra Private Access, Microsoft Entra Internet Access will begin to rollout on October 1, 2024. This is following a 90-day trial period that began with General Availability on July 1st, 2024. Learn more
Review tenant accessed by users in your organization. Tenant restriction policy can be used to block access to unsanctioned tenants.
1 item
Search
Usage status
Resource tenant ID
User count
Device count
Last activity
Rarely used
bb755851-a1be-4075-9aa7-2863bc0ecb29
1
1
11/13/2024, 03:27 PM
Cross-tenant access
Total distinct tenan
Rarely used tenants
Users
Devices
12K
295
249
44
30



Add filter | Show dates as: Local | Date range: Last 7 days | Service : Global Secure Access | Category : All | Activity : All | Reset filters

Directory

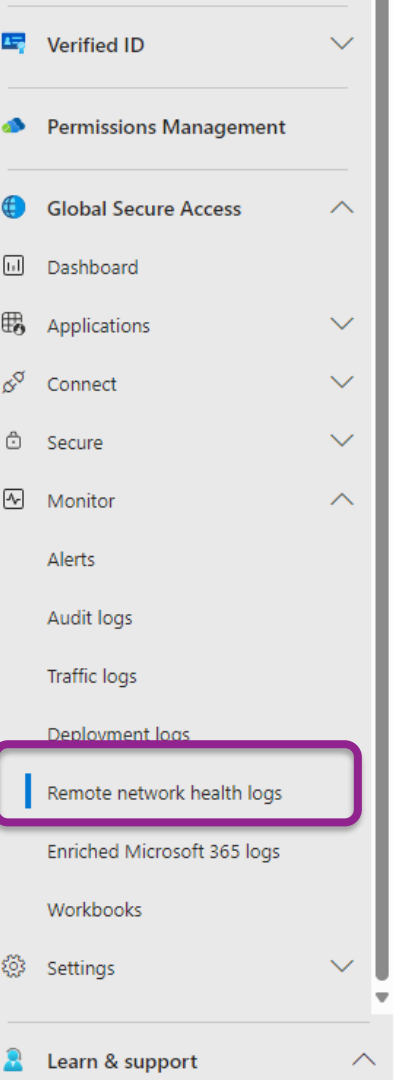
Date ↓	Service	Category	Activity	Status	Statu
11/12/24, 11:16:40 PM	Global Secure Access	PolicyManagement	Update Filtering Profile	Success	Upda
11/12/24, 11:16:17 PM	Global Secure Access	PolicyManagement	Update Filtering Policy	Success	Delet
11/12/24, 11:15:35 PM	Global Secure Access	PolicyManagement	Update Filtering Profile	Success	Add F
11/12/24, 11:15:35 PM	Global Secure Access	PolicyManagement	Create Filtering Policy	Success	Add F
11/12/24, 11:14:55 PM	Global Secure Access	PolicyManagement	Update Filtering Profile	Success	Add F
11/12/24, 11:14:55 PM	Global Secure Access	PolicyManagement	Create Filtering Policy	Success	Add F
11/12/24, 11:14:27 PM	Global Secure Access	PolicyManagement	Create Filtering Policy	Success	Add F
11/7/24, 10:50:17 PM	Global Secure Access	PolicyManagement	Update Filtering Policy P...	Success	Upda
11/7/24, 10:46:53 PM	Global Secure Access	PolicyManagement	Update Filtering Policy P...	Success	Upda
11/7/24, 10:44:57 PM	Global Secure Access	PolicyManagement	Update Filtering Profile	Success	Add F
11/7/24, 10:44:57 PM	Global Secure Access	PolicyManagement	Create Filtering Policy	Success	Add F
11/7/24, 10:44:34 PM	Global Secure Access	PolicyManagement	Update Filtering Policy P...	Success	Upda
11/7/24, 10:35:52 PM	Global Secure Access	PolicyManagement	Update Filtering Profile	Success	Add F
11/7/24, 10:35:52 PM	Global Secure Access	PolicyManagement	Create Filtering Policy	Success	Add F
11/7/24, 10:29:49 PM	Global Secure Access	PolicyManagement	Create Filtering Policy	Success	Add F
11/7/24, 10:23:20 PM	Global Secure Access	PolicyManagement	Delete Filtering Policy	Success	Delet
11/7/24, 10:23:00 PM	Global Secure Access	PolicyManagement	Update Filtering Policy	Success	Delet
11/7/24, 1:16:36 PM	Global Secure Access	PolicyManagement	Update Private Access P...	Success	Upda

Download | Refresh | Columns | Got feedback?

All Connections	Internet Access	Private Access
17K	15K	6

Timespan : Last 24 hours | Add filter

Created date time ↓	Traffic type	Destination FQDN	User principal name	Action	Source IP	Sent bytes	Received bytes
11/13/2024, 09:13 PM	Microsoft 365	microsoft-my.share...	Dash@idefix365.no	Allow	51.13.50.34	184 bytes	665 bytes
11/13/2024, 09:13 PM	Microsoft 365	spo-ring.msedge.net	Dash@idefix365.no	Allow	51.13.50.34	0 bytes	0 bytes
11/13/2024, 09:13 PM	Microsoft 365	spo-ring.msedge.net	Dash@idefix365.no	Allow	51.13.50.34	0 bytes	0 bytes
11/13/2024, 09:13 PM	Microsoft 365	graph-next.fp.mea...	Dash@idefix365.no	Allow	51.13.50.34	0 bytes	0 bytes
11/13/2024, 09:13 PM	Microsoft 365	spo-ring-fallback....	Dash@idefix365.no	Allow	51.13.50.34	0 bytes	0 bytes
11/13/2024, 09:13 PM	Microsoft 365	outlook.office365.c...	Dash@idefix365.no	Allow	51.13.50.34	0 bytes	0 bytes
11/13/2024, 09:13 PM	Microsoft 365	outlook.office365.c...	Dash@idefix365.no	Allow	51.13.50.34	162 bytes	535 bytes
11/13/2024, 09:13 PM	Microsoft 365	outlook.office365.c...	Dash@idefix365.no	Allow	51.13.50.34	157 bytes	535 bytes
11/13/2024, 09:13 PM	Microsoft 365	microsoft.sharepoi...	Dash@idefix365.no	Allow	51.13.50.34	15 MB	1.74 KB
11/13/2024, 09:13 PM	Internet	westeurope-share...	Dash@idefix365.no	Allow	51.13.50.34	1.39 KB	6.63 KB
11/13/2024, 09:13 PM	Internet	advmetric-black.pr...	Dash@idefix365.no	Allow	51.13.50.34	9.01 KB	13.08 KB
11/13/2024, 09:13 PM	Microsoft 365	microsoft.sharepoi...	Dash@idefix365.no	Allow	51.13.50.34	0 bytes	0 bytes
11/13/2024, 09:13 PM	Microsoft 365	microsoft.sharepoi...	Dash@idefix365.no	Allow	51.13.50.34	207 bytes	15.99 KB
11/13/2024, 09:13 PM	Microsoft 365	login.microsoftonli...	Dash@idefix365.no	Allow	51.13.50.34	0 bytes	0 bytes
11/13/2024, 09:13 PM	Internet	westeurope-share...	Dash@idefix365.no	Allow	51.13.50.34	1.4 KB	6.63 KB
11/13/2024, 09:12 PM	Internet	westeurope-share...	Dash@idefix365.no	Allow	51.13.50.34	1.39 KB	6.66 KB



Created date time ↓	Source IP	Destination IP	Status	Description	BGP routes advertised count	Sent bytes	Rece

No data

Microsoft Security Copilot

Monitor data consumption and bandwidth usage

- Show the top 5 users with the highest data consumption in the last day.
- List the top 10 accessed applications names in the last week based on network traffic logs.

NIC REBEL EDITION

Microsoft Security Copilot

Analyze user application access patterns

- List all applications names that user sarah.manager@woodgrovebank.com has accessed in the last 24 hours based on network traffic logs.

NIC REBEL EDITION

Microsoft Security Copilot

Monitor cross-tenant access and external connections

- Show all cross-tenant traffic to tenant aaaabbbb-0000-cccc-1111-dddd2222eeee in the last 7 days based on network traffic logs.

NIC REBEL EDITION

We have ..

- Learned the difference between GSA traffic profiles
- Secured M365 traffic with Global Secure access and Conditional Access
- Blocked a public website with Internet Access web content filtering
- Created a tunnel to our “on-premises” infrastructure

NIC REBEL EDITION