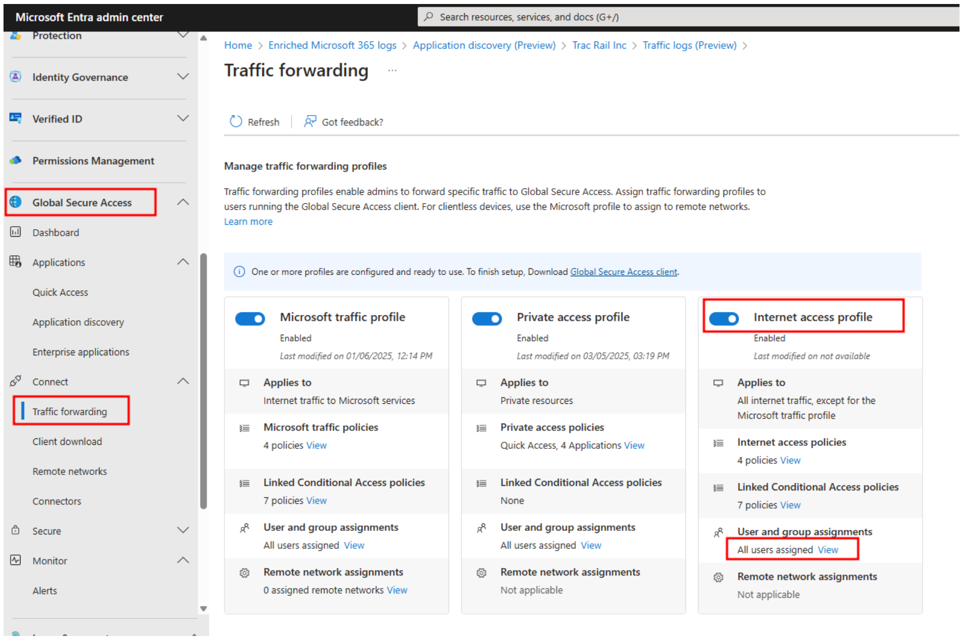
Microsoft Entra Internet access :

1. Login to the Microsoft Entra admin center. From the “Global Secure Access”. Click on “Connect”>” Traffic Forwarding” and turn on Internet access Profile. Also Assign users.



Traffic forwarding ...

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 01/06/2025, 12:14 PM

- Applies to: Internet traffic to Microsoft services
- Microsoft traffic policies: 4 policies View
- Linked Conditional Access policies: 7 policies View
- User and group assignments: All users assigned View
- Remote network assignments: 0 assigned remote networks View

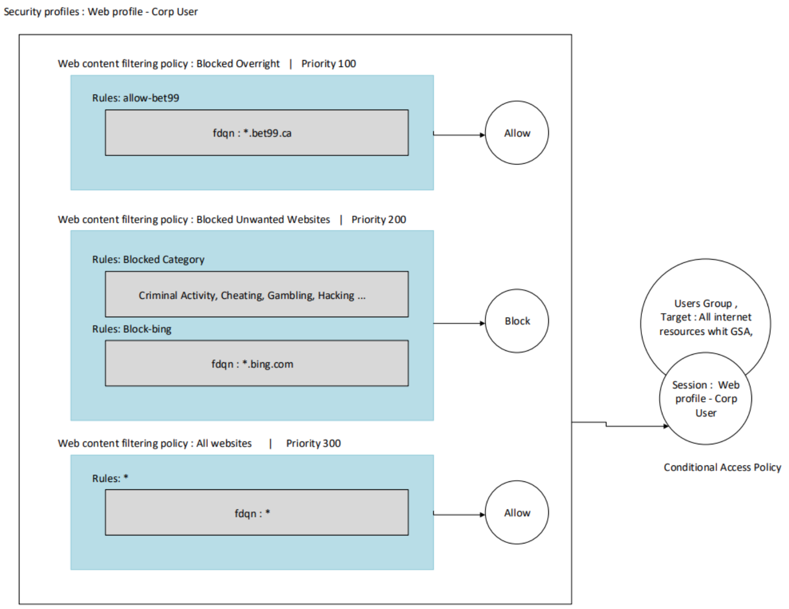
Private access profile
Enabled
Last modified on 03/05/2025, 03:19 PM

- Applies to: Private resources
- Private access policies: Quick Access, 4 Applications View
- Linked Conditional Access policies: None
- User and group assignments: All users 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: 7 policies View
- User and group assignments: All users assigned View
- Remote network assignments: Not applicable

How Profiles, Policy, rules and Conditional access work:



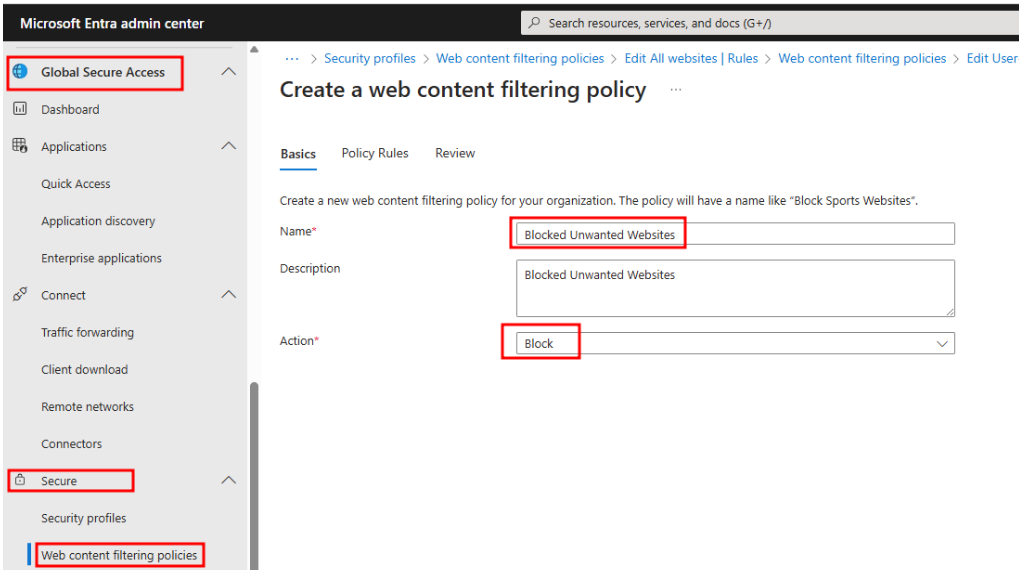
Security profiles : Web profile - Corp User
Web content filtering policy : Blocked Overright | Priority 100
Rules: allow-bet99
fdqn : *.bet99.ca
Allow
Web content filtering policy : Blocked Unwanted Websites | Priority 200
Rules: Blocked Category
Criminal Activity, Cheating, Gambling, Hacking ...
Rules: Block-bing
fdqn : *.bing.com
Block
Web content filtering policy : All websites | Priority 300
Rules: *
fdqn : *
Allow
Users Group , Target : All internet resources whit GSA,
Session : Web profile - Corp User
Conditional Access Policy

2. Web Content filtering policies:

For the most use case, Crate three content filtering policy

- Allow All websites (built in)
- Block policy (for blocking categories and interested fdqn)

  Select “Web content filtering policies” under Global Secure Access. And create new policy


Microsoft Entra admin center
Search resources, services, and docs (G+/)
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
… > Security profiles > Web content filtering policies > Edit All websites | Rules > Web content filtering policies > Edit User
Basics
Policy Rules
Review

Create a web content filtering policy …

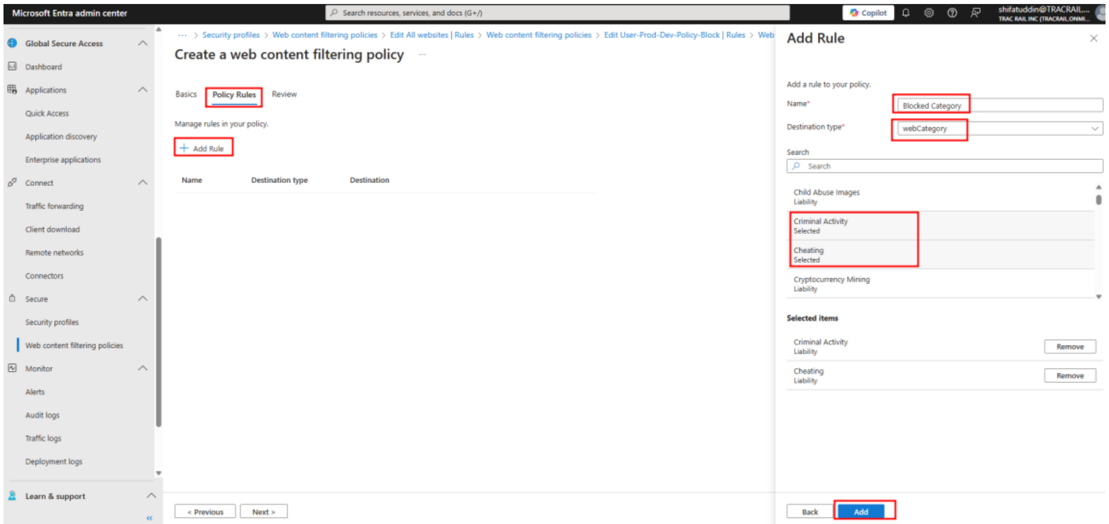
Create a new web content filtering policy for your organization. The policy will have a name like "Block Sports Websites".

Name* Blocked Unwanted Websites

Description Blocked Unwanted Websites

Action* Block

Now click on “Policy Rules” tab. Click on “Add rule”. Give it a name choose “webCategory” as Destination Type. Select all the categories to block and add.



Create a web content filtering policy …

Manage rules in your policy.

Name	Destination type	Destination

Add Rule

Add a rule to your policy.

Name* Blocked Category

Destination type* webCategory

Search

Child Abuse Images
Liability

Criminal Activity
Selected

Cheating
Selected

Cryptocurrency Mining
Liability

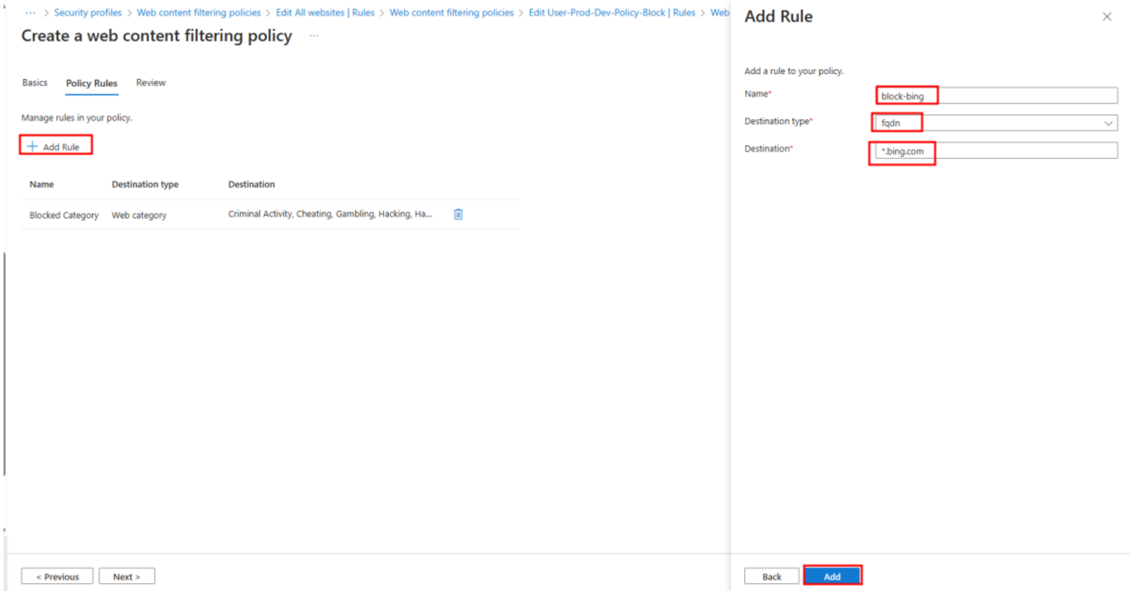
Selected items

Criminal Activity
Liability
Remove

Cheating
Liability
Remove

Back Add

For non-Category sites add another rule and select Destination type as fdqn. For example we blocked bing.com.



… > Security profiles > Web content filtering policies > Edit All websites | Rules > Web content filtering policies > Edit User-Prod-Dev-Policy-Block | Rules > Web

Create a web content filtering policy …

Basics | Policy Rules | Review

Manage rules in your policy.

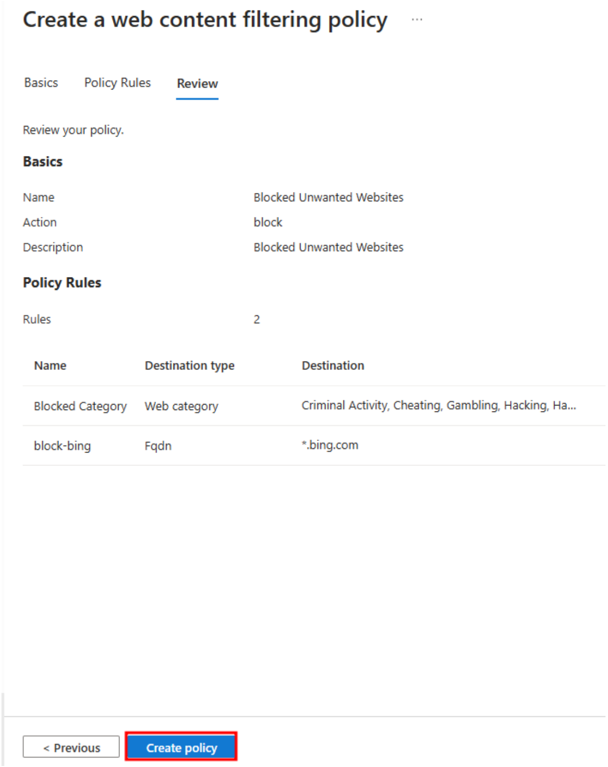
Name	Destination type	Destination
Blocked Category	Web category	Criminal Activity, Cheating, Gambling, Hacking, Ha...

Add Rule

Add a rule to your policy.

Name*	block-bing
Destination type*	fqdn
Destination*	*.bing.com

Review and create the policy



Create a web content filtering policy …

Basics | Policy Rules | Review

Review your policy.

Basics

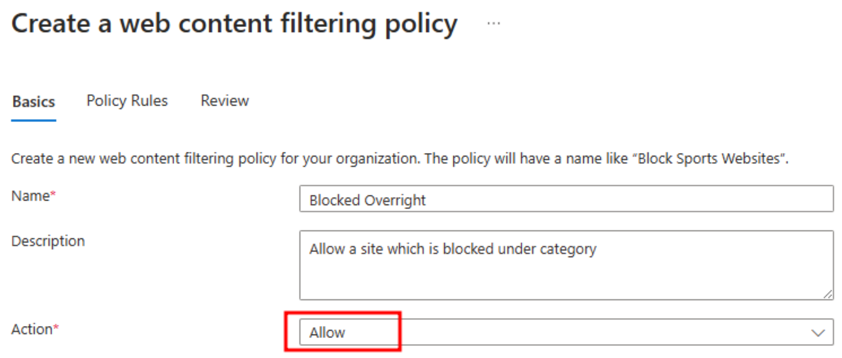
Name	Blocked Unwanted Websites
Action	block
Description	Blocked Unwanted Websites

Policy Rules

Rules 2

Name	Destination type	Destination
Blocked Category	Web category	Criminal Activity, Cheating, Gambling, Hacking, Ha...
block-bing	Fqdn	*.bing.com

- Blocked overright ; create another policy to allow a site from blocked category



Create a web content filtering policy ···

Basics Policy Rules Review

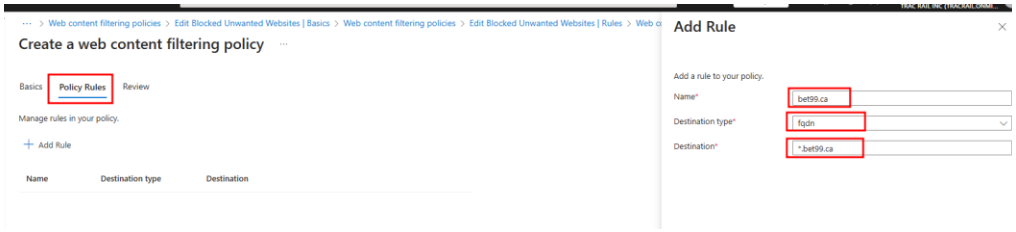
Create a new web content filtering policy for your organization. The policy will have a name like "Block Sports Websites".

Name* Blocked Overright

Description Allow a site which is blocked under category

Action* Allow

On the policy Rules add the fdqn to allow



··· > Web content filtering policies > Edit Blocked Unwanted Websites | Basics > Web content filtering policies > Edit Blocked Unwanted Websites | Rules > Web c

Create a web content filtering policy ···

Basics Policy Rules Review

Manage rules in your policy.

+ Add Rule

Name	Destination type	Destination

Add Rule

Add a rule to your policy.

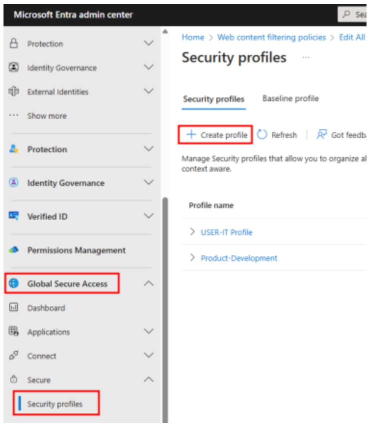
Name* bet99.ca

Destination type* fqdn

Destination* *.bet99.ca

3. Security profiles:

After creating all the policies, Click on Security profiles and create new profile.



Home > Web content filtering policies > Edit All

Security profiles ···

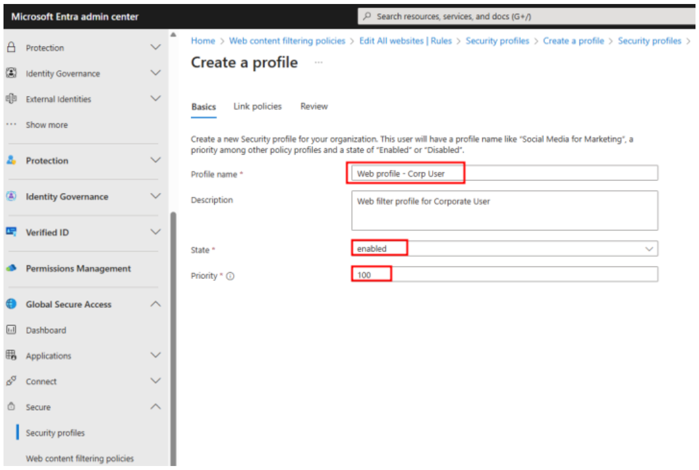
Security profiles Baseline profile

+ Create profile Refresh Got feedb

Manage Security profiles that allow you to organize al context aware.

Profile name
USER-IT Profile
Product-Development

Give a name for the profile, add description and set priority.


Microsoft Entra admin center
Search resources, services, and docs (G+/)
Protection
Identity Governance
External Identities
Show more
Protection
Identity Governance
Verified ID
Permissions Management
Global Secure Access
Dashboard
Applications
Connect
Secure
Security profiles
Web content filtering policies
Home > Web content filtering policies > Edit All websites | Rules > Security profiles > Create a profile > Security profiles >
Basics
Link policies
Review

Create a profile

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".

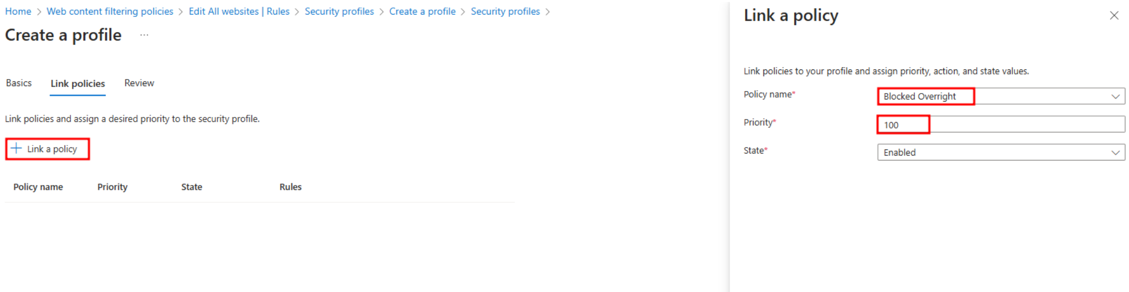
Profile name * Web profile - Corp User

Description Web filter profile for Corporate User

State * enabled

Priority * 100

Move to Linked policy, click on "Link a policy" > add existing policy. Select "Blocked Overright" policy and set priority to 100 and add


Home > Web content filtering policies > Edit All websites | Rules > Security profiles > Create a profile > Security profiles >
Basics
Link policies
Review
+ Link a policy

Create a profile

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

Policy name	Priority	State	Rules

Link a policy

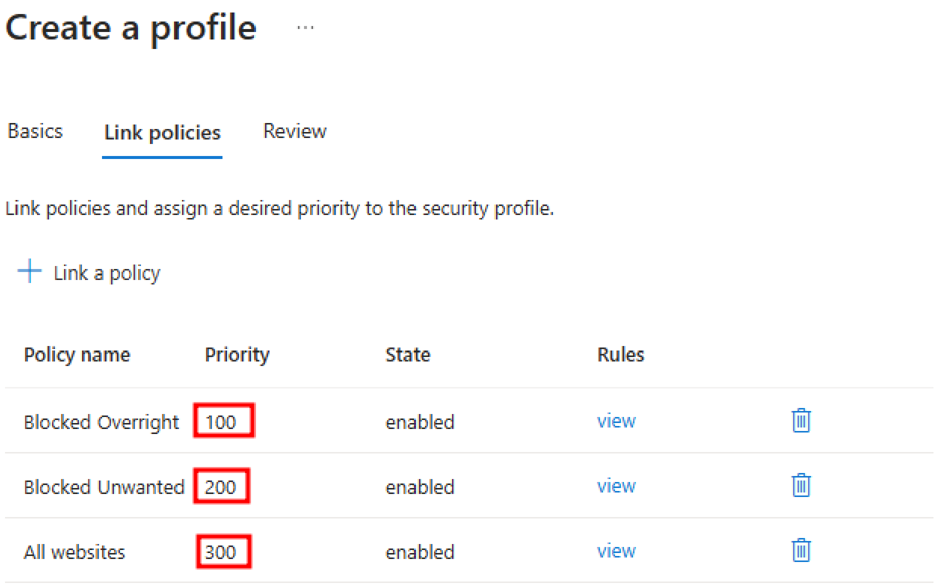
Link policies to your profile and assign priority, action, and state values.

Policy name* Blocked Overright

Priority* 100

State* Enabled

In the same way link "Blocked Unwanted" with 200 priority and "All website" with 300 priorities.



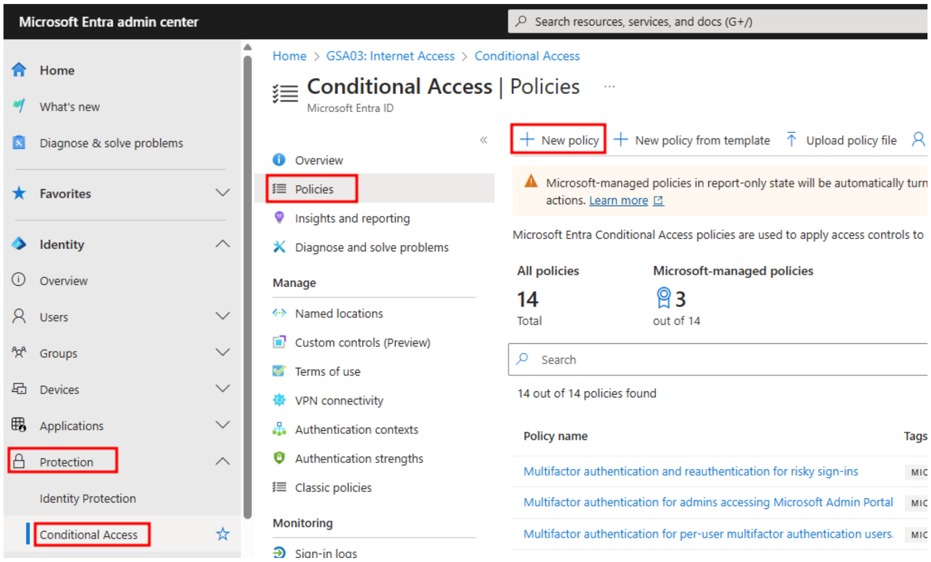
Create a profile

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

Policy name	Priority	State	Rules	
Blocked Overright	100	enabled	view	🗑
Blocked Unwanted	200	enabled	view	🗑
All websites	300	enabled	view	🗑

4. Conditional Access Policy:

On the Entra Admin Center, Click on Protection > Conditional Access > policies. Then create New policy



Microsoft Entra admin center

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

Home
What's new
Diagnose & solve problems
Favorites
Identity
Overview
Users
Groups
Devices
Applications
Protection
Identity Protection
Conditional Access

Home > GSA03: Internet Access > 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

+ New policy   + New policy from template   Upload policy file

Microsoft-managed policies in report-only state will be automatically turn actions. Learn more

Microsoft Entra Conditional Access policies are used to apply access controls to

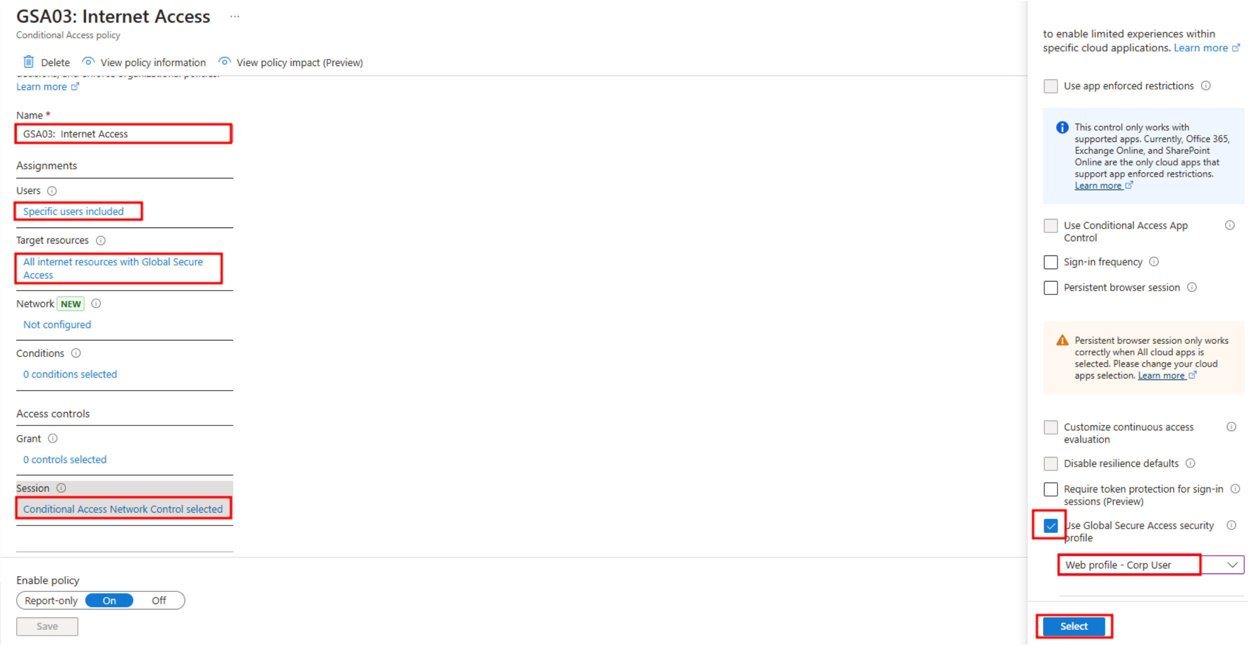
All policies	Microsoft-managed policies
14 Total	3 out of 14

Search

14 out of 14 policies found

Policy name	Tags
Multifactor authentication and reauthentication for risky sign-ins	MIC
Multifactor authentication for admins accessing Microsoft Admin Portal	MIC
Multifactor authentication for per-user multifactor authentication users.	MIC

Give the policy a name. add targeted user group, set target resource as “All internet resources with GSA” and Grant access. From the Session select “Web profile – Crop User” as Global Security profile. Finally Enable the Policy.



GSA03: Internet Access ...

Conditional Access policy

Delete   View policy information   View policy impact (Preview)

Learn more

Name *

GSA03: Internet Access

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

Conditional Access Network Control selected

Enable policy

Report-only [✓ On] Off

Save

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)

☑ Use Global Secure Access security profile

Web profile - Corp User

Select