

# BREAKING BOUNDARIES

Microsoft SSE and  
SASE Evolution



Friday, January 31, 2025 | 11:30 AM - 1:00 PM | @ Foundation For A Healthy Kentucky



Security

### Specialist

Cloud Security

Identity and Access

Management

Threat Protection

Information Protection and

Governance

# Josh Gatewood

- Certs
  - Azure Admin Associate
  - Identity and Access Admin Associate
  - Security Admin Associate
  - Azure Security Engineer Associate
  - Cloud Fundamentals
  - Security, Compliance and Identity Fundamentals
  - Information Protection and Compliance Associate
  - GCP Infrastructure Admin
  - MTA: Cloud Associate

# Security Boundaries



Identity



Workstation



Network



# Secure Access Service Edge



## Software-defined wide area network (SD-WAN)

A software-defined wide area network is an overlay architecture that uses routing or switching software to create virtual connections between [endpoints](#)—both physical and logical. SD-WANs provide near-unlimited paths for user traffic, which optimizes the user experience, and allows for powerful flexibility in encryption and policy management.



## Firewall as a service (FWaaS)

Firewall as a service moves firewall protection to the cloud instead of the traditional network perimeter. This enables organizations to securely connect a remote, mobile workforce to the corporate network, while still enforcing consistent security policies that reach beyond the organization's geographic footprint.



## Secure web gateway (SWG)

A secure web gateway is a web security service that filters unauthorized traffic from accessing a particular network. The goal of a SWG is to zero in on threats before they penetrate a virtual perimeter. A SWG accomplishes this by combining technologies like malicious code detection, [malware](#) elimination, and URL filtering.



## Zero Trust Network Access (ZTNA)

Zero Trust Network Access is a set of consolidated, cloud-based technologies that operates on a framework in which trust is never implicit and access is granted on a need-to-know, least-privileged basis across all users, devices, and applications. In this model, all users must be authenticated, authorized, and continuously validated before being granted access to company private applications and data. ZTNA eliminates the poor user experience, operational complexities, costs, and risk of a traditional VPN.



## Cloud access security broker (CASB)

A cloud access security broker is a SaaS application that acts as a security checkpoint between on-premises networks and cloud-based applications and enforces data security policies. A [CASB](#) protects corporate data through a combination of prevention, monitoring, and mitigation techniques. It can also identify malicious behavior and warn administrators about compliance violations.



## Centralized and unified management

A modern SASE platform allows IT administrators to manage SD-WAN, SWG, CASB, FWaaS, and ZTNA through centralized and unified management across networking and security. This frees IT team members to focus their energy in other more pressing areas and boosts the user experience for the organization's hybrid workforce.

# Microsoft Zero Trust Capability Mapping to NIST ZT Architecture

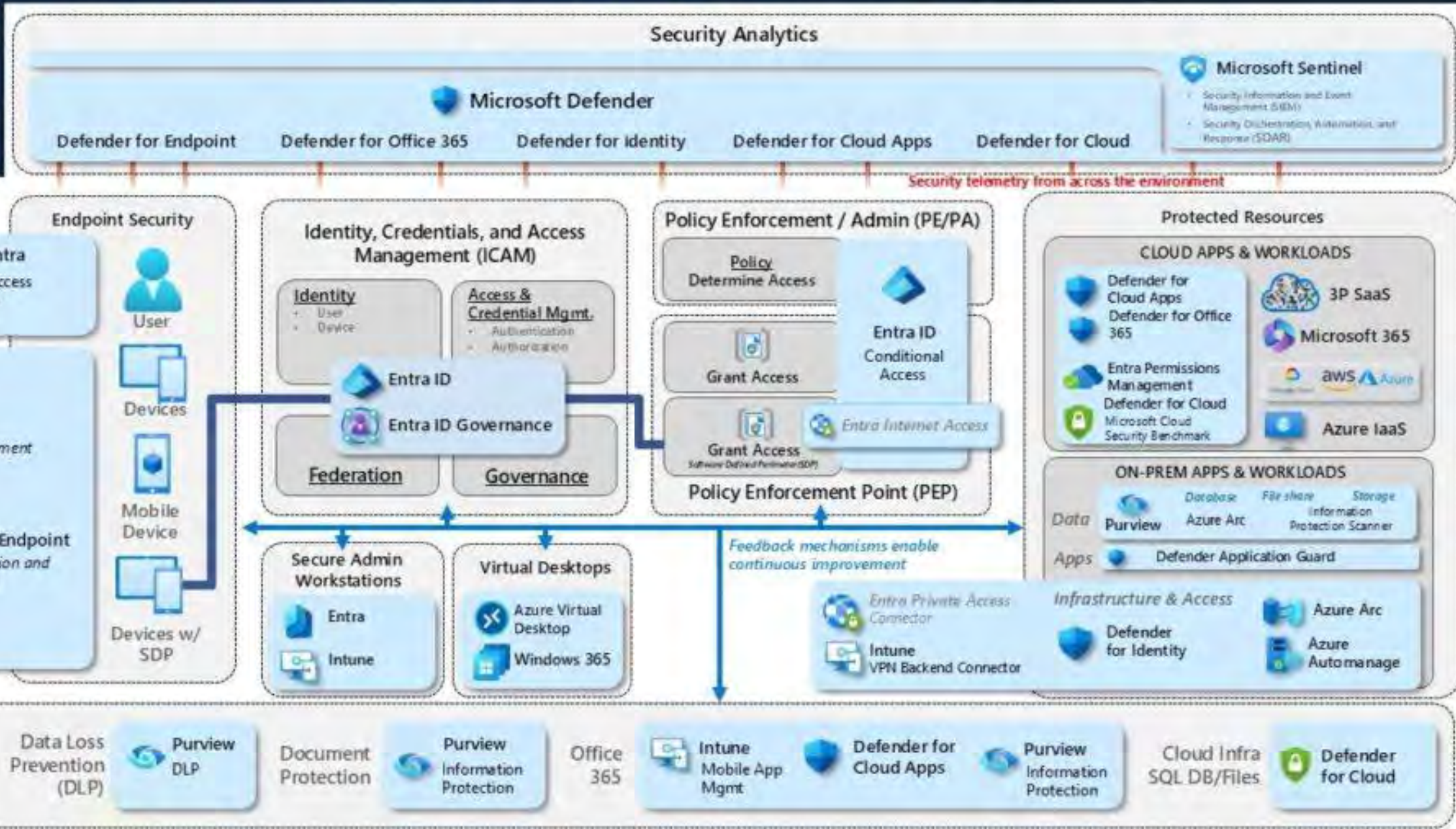
Key

**NIST Area**

**NIST Sub-Area**

• Sub-Area

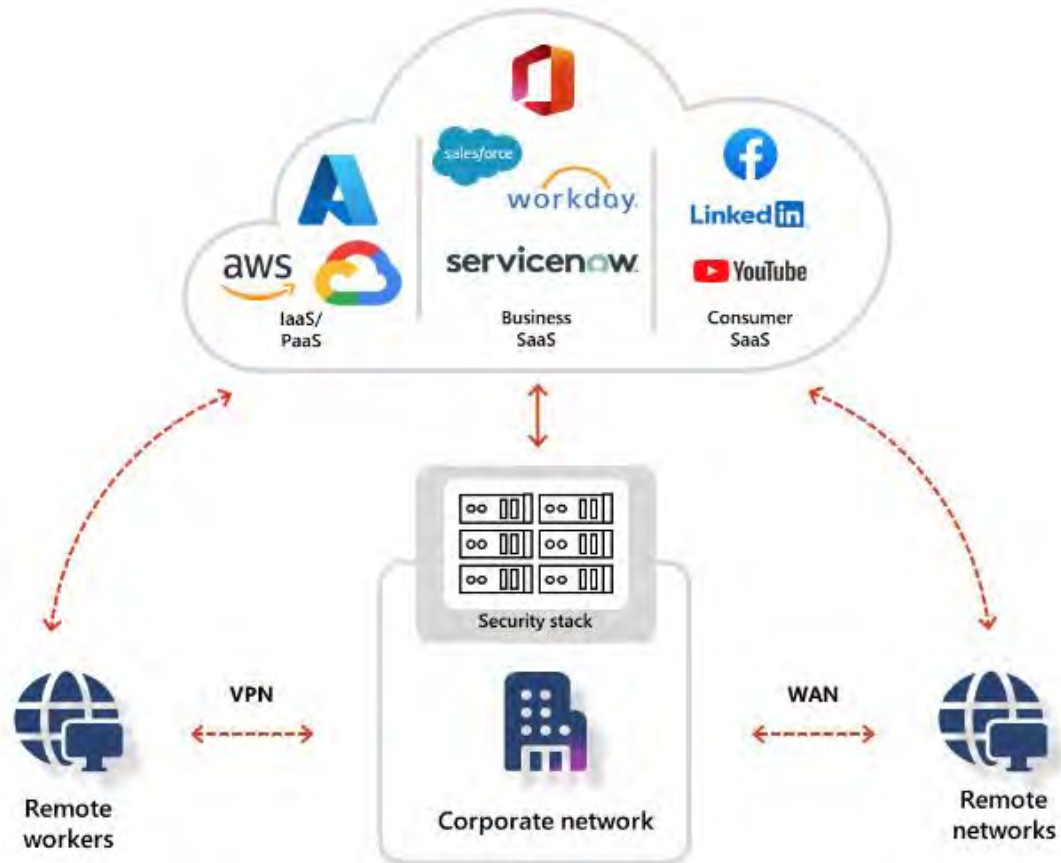
**Microsoft Service**

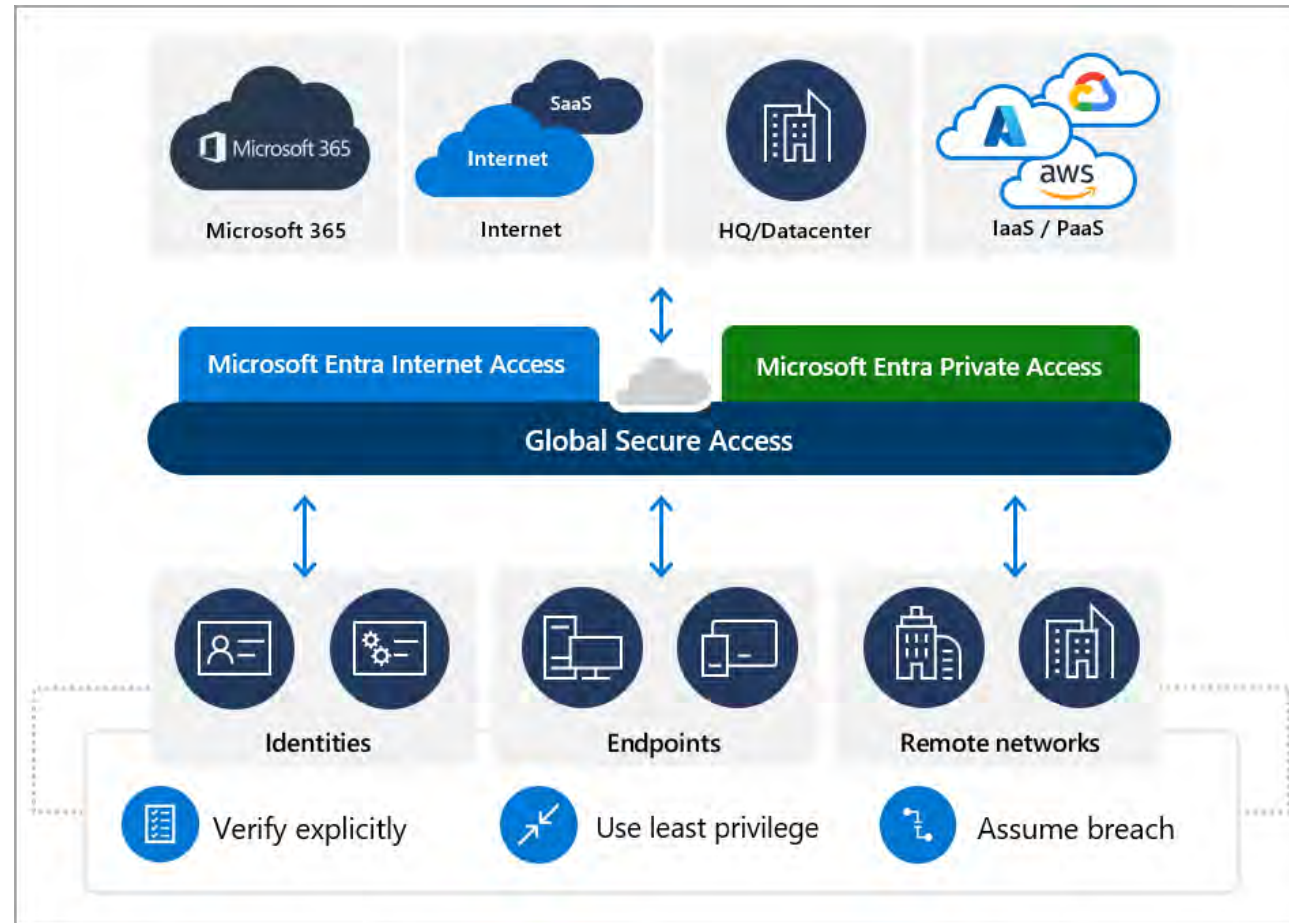


All this for Zero Trust?



# Secure Service Edge

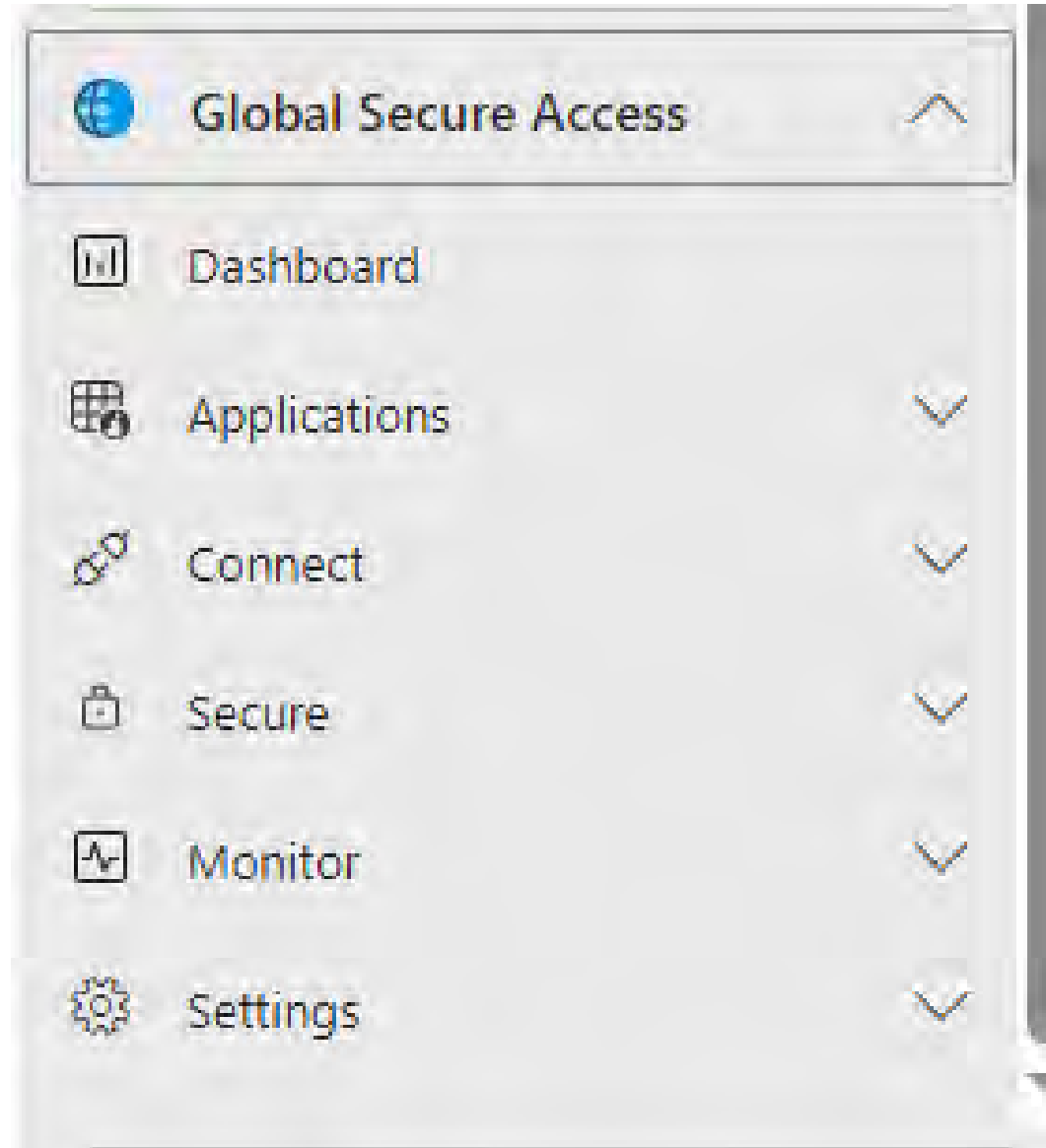




# Global Secure Access





# Global Secure Access





# Traffic Forwarding Profiles


**Microsoft traffic profile**  
Enabled  
*Last modified on 05/20/2024, 01:34 PM*

 **Applies to**  
Internet traffic to Microsoft services


 **Microsoft traffic policies**  
3 policies [View](#)


 **Linked Conditional Access policies**  
1 policy [View](#)


 **User and group assignments**  
All users assigned [View](#)


 **Remote network assignments**  
1 assigned remote networks [Edit](#)


**Private access profile**  
Enabled  
*Last modified on 09/16/2024, 10:29 AM*

 **Applies to**  
Private resources


 **Private access policies**  
Quick Access, 2 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**  
3 policies [View](#)

 **Linked Conditional Access policies**  
2 policies [View](#)

 **User and group assignments**  
All users assigned [View](#)

 **Remote network assignments**  
Not applicable

# M365 Access Profile

## Policies & rules (Microsoft 365 profile)

Traffic Profile

Global Secure Access preview acquires TCP traffic. UDP support will be added in the future. Remote networks acquire IP-identifiable traffic only.

① Please note that we are working on acquiring additional Microsoft 365 traffic. Complete Office 365 URLs and IP address ranges can be found here: [Office 365 URLs and IP address ranges](#)


Policy	Enable/Disable	Destinati...	Destination	Ports	Category	Proto...	Action
Exchange Online	<input checked="" type="checkbox"/>						
Rules							
		Fqdn	outlook.office.com, outlook.office36i	80, 443	Optimized	Tcp	Forward
		IpSubnet	13.107.6.152/31, 13.107.18.10/31, 13	80, 443	Optimized	Tcp	Forward
		Fqdn	*.outlook.com	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	autodiscover.*.onmicrosoft.com	80, 443	Default	Tcp	Forward
SharePoint Online and OneDrive for Business	<input checked="" type="checkbox"/>						
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	ssw.live.com, storage.live.com	443	Default	Tcp	Forward
		Fqdn	*.search.production.apac.trafficmana	443	Default	Tcp	Forward
		Fqdn	*.wms.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	<input checked="" type="checkbox"/>						
Rules							
		Fqdn	*.auth.microsoft.com, *.msftidentity.c	80, 443	Allow	Tcp	Forward
		IpSubnet	20.20.32.0/19, 20.190.128.0/18, 20.2	80, 443	Allow	Tcp	Forward
		Fqdn	account.live.com, login.live.com	443	Default	Tcp	Forward

# Target Resources – Conditional Access

Control access based on all or specific network access traffic, cloud apps or actions.


[Learn more](#) 

Select what this policy applies to

Global Secure Access (Preview) 

Select the traffic profiles this policy applies to



0 selected 

- Microsoft 365 traffic
- Internet traffic
- Private traffic

# Internet Access Profile – Web Filtering

Manage web content filtering policies.

Policy name	Rules	Created on	Last Modified	Action
<a href="#">All websites</a>	1	02/14/2024, 05:55 AM	02/14/2024, 05:55 AM	allow
<a href="#">Blocked Categories</a>	1	02/29/2024, 11:16 AM	02/29/2024, 11:16 AM	block
<a href="#">block espn</a>	2	05/13/2024, 01:39 PM	05/20/2024, 01:42 PM	block
<a href="#">block social</a>	1	05/13/2024, 01:55 PM	05/13/2024, 01:55 PM	block
<a href="#">Platform SSO</a>	2	07/16/2024, 02:32 PM	07/16/2024, 02:32 PM	block

## 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
▼ <a href="#">Block Social</a>	100	2			enabled	05/13/2024
block espn	101		web filtering	block		
block social	102		web filtering	block		
▼ <a href="#">Block 2</a>	101	4			enabled	05/20/2024
block espn	100		web filtering	block		
Blocked Categories	105		web filtering	block		
block social	110		web filtering	block		
All websites	500		web filtering	allow		

# Security Profile – Internet Access

Use Global Secure Access security profile



Block 2

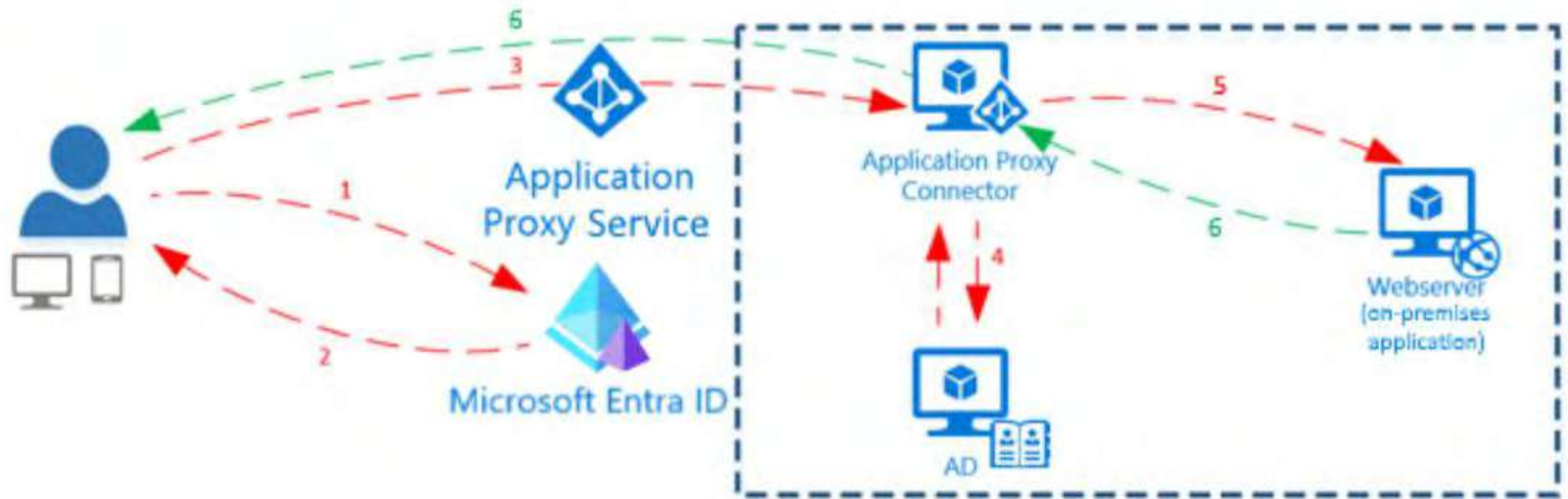


Block Social

Block 2

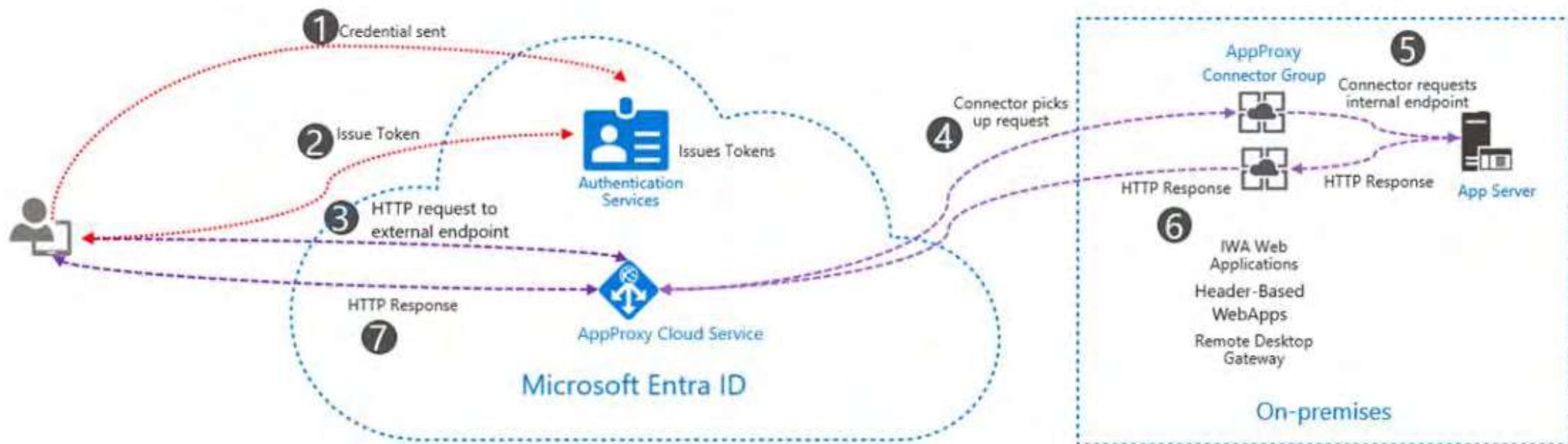
Integrate with Conditional Access

# Microsoft Private Access - Entra App Proxy





# User Experience with App Proxy





# Quick Access Configuration

[Home](#) >


## Edit Quick Access configuration ...

 [Edit application settings](#) |  [Got feedback?](#)


 Get early access to Quick Access private preview features that further simplify VPN replacement. [Submit a request to join the private preview](#) 


Name  \*

Connector Group 

 We recommend at least two active connectors in selected group 'ServerAccess'. [Click here to download a connector or manage your connector groups.](#)

### Application Segment

 Add Quick Access application segment

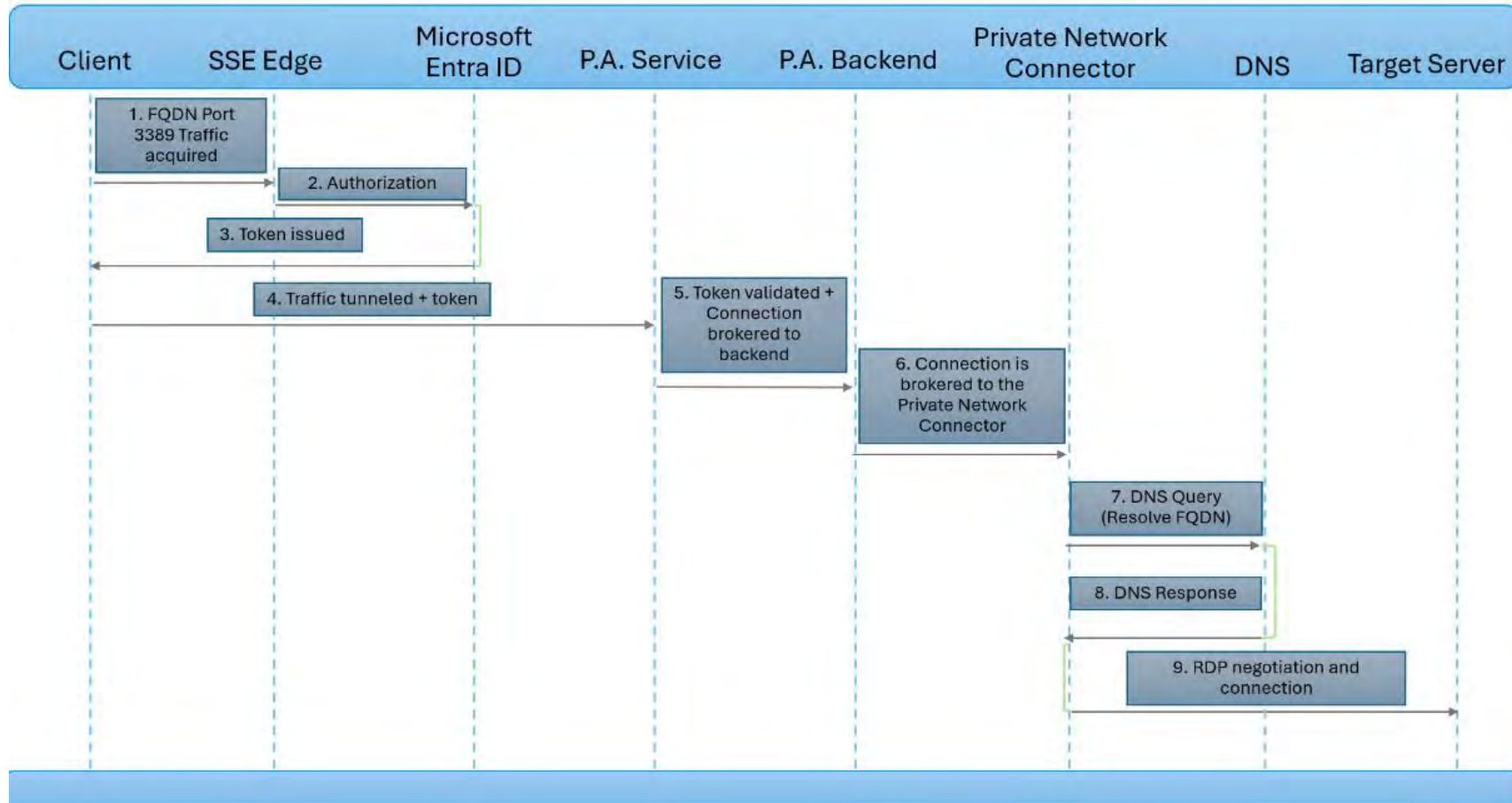
Destination type	Destination	Ports	Delete
<a href="#">IP address range (CIDR)</a>	192.168.100.1/24	80,443,3389	

RDP! RDP! RDP!

The image shows a web browser window titled "Private Access Applications - Sign In" displaying a "CONTOSO demo" sign-in page. The page has a dark blue header with the "CONTOSO demo" logo and a main white area with the heading "Pick an account". Two account options are listed: "JoshAdmin" with email "JoshAdmin@M365t29811314.onmicrosoft.com" and status "Connected to Windows", and "Use another account". A "Back" button is at the bottom right of the sign-in area. At the bottom of the page, there are links for "Terms of use" and "Privacy & cookies".

Overlaid on the sign-in page are several overlapping "Remote Desktop Connection" dialog boxes. The most prominent one in the foreground shows "Connecting to: 192.168.100.10" with a green progress bar and a "Cancel" button. Below it, another dialog box shows "Initiating remote connection..." with "Show Options", "Connect", and "Help" buttons. A third dialog box is partially visible behind the others, showing network protocol settings like "Version 4 (TCP/IPv4)" and "Adapter Multiplexor Protocol".

# RDP Auth Flow



# GSA Client

## Windows



Windows 10/11

[Download Client](#)

System requirements

- Windows 10/11
- Microsoft Entra joined
- Local admin permissions

## 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.

## macOS PREVIEW



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

# GSA Client Analytics

The screenshot displays the 'Global Secure Access Client - Advanced diagnostics' window. The 'Forwarding profile' tab is active, showing details for a specific profile. Below the details, there is a 'Refresh details' button. The 'Rules' section is also visible, listing three rule categories: 'Microsoft 365 rules', 'Private access rules', and 'Internet access rules'. Each rule category has a dropdown arrow on the right side.

Global Secure Access Client - Advanced diagnostics

Overview Health check **Forwarding profile** Hostname acquisition Traffic ...

### Forwarding profile details

View all the rules applied to this client. [Learn more](#)

Forwarding profile ID	CPV:RV:2024-09-16T14:31:45.0063787Z_CPLM:2...
Forwarding profile last updated	10/9/2024 5:50:58 AM

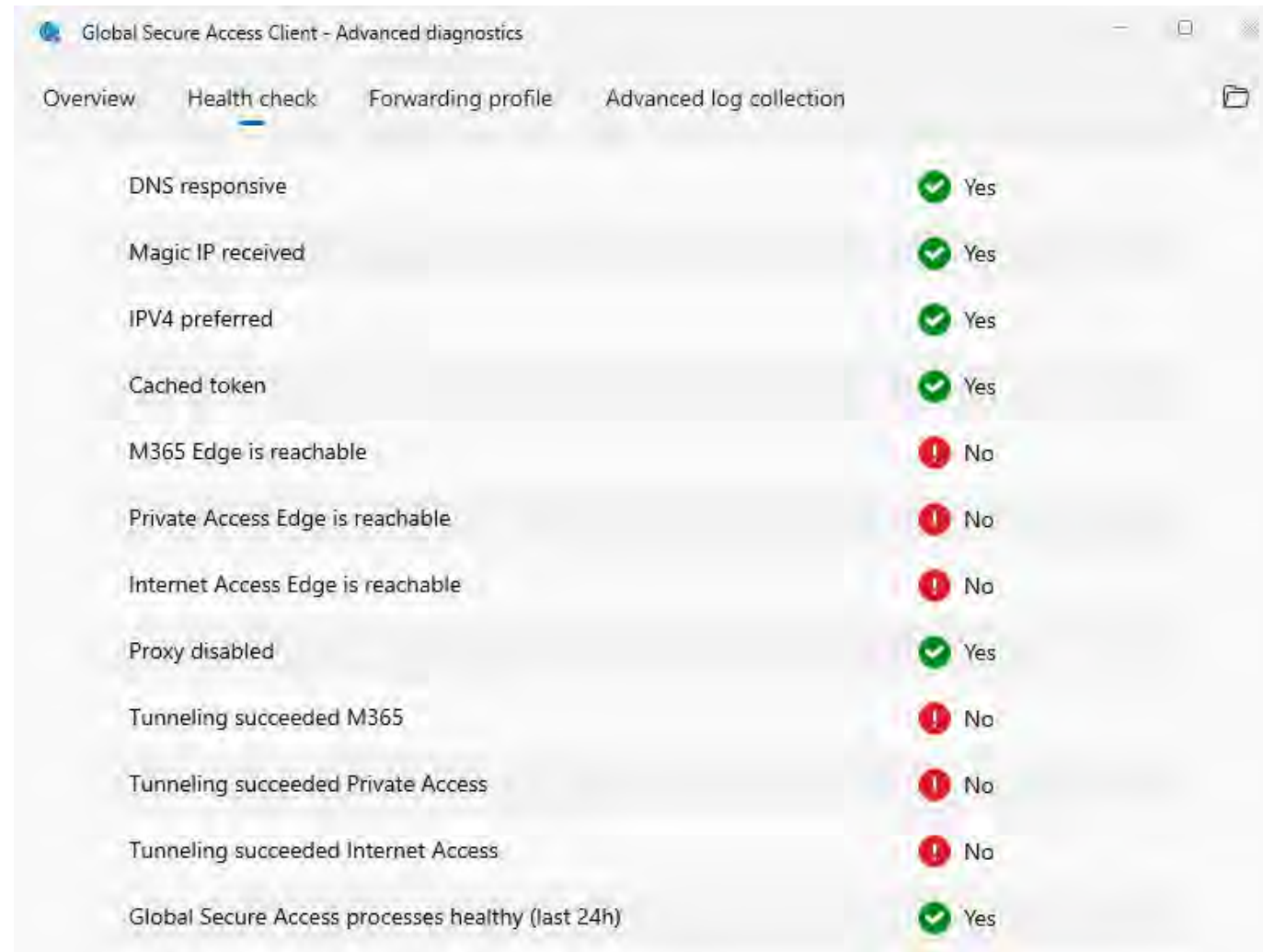
[Refresh details](#)

### Rules

[Add filter](#) [Columns](#)

- Microsoft 365 rules
- Private access rules
- Internet access rules

# GSA Health Check



The screenshot shows the 'Global Secure Access Client - Advanced diagnostics' window with the 'Health check' tab selected. The table below lists various diagnostic items and their status.

Diagnostic Item	Status
DNS responsive	Yes
Magic IP received	Yes
IPV4 preferred	Yes
Cached token	Yes
M365 Edge is reachable	No
Private Access Edge is reachable	No
Internet Access Edge is reachable	No
Proxy disabled	Yes
Tunneling succeeded M365	No
Tunneling succeeded Private Access	No
Tunneling succeeded Internet Access	No
Global Secure Access processes healthy (last 24h)	Yes

# Advanced Log Collection





# Familiar Error messages



## ZTNA Network Access Client -- Private

Sorry, but we're having trouble signing you in.

AADSTS50105: Your administrator has configured the application ServerAccess ('8d7c1762-ead2-4ee2-b5ed-b8e61306098f') to block users unless they are specifically granted ('assigned') access to the application. The signed in user 'JoshAdmin@M365t29811314.onmicrosoft.com' is blocked because they are not a direct member of a group with access, nor had access directly assigned by an administrator. Please contact your administrator to assign access to this application.

Contoso



josh\_patriot@m365t29811314.onmicrosoft.com

## You cannot access this right now

Your sign-in was successful but does not meet the criteria to access this resource. For example, you might be signing in from a browser, app, or location that is restricted by your admin.

[More details](#)

OK

# Log Activity



Home > **Traffic logs**

Download Refresh Columns Got feedback?

All Connections 1.1K | Internet Access 10 | Private Access 28 | Microsoft 365 Access 1K

Timespan: Last 24 hours Add filter

Created date time ↓	Traffic type	Destination FQDN	User principal name	Action
12/12/2023, 07:39 PM	Microsoft 365	substrate.office.com	Josh_Patriot@M365t2...	Allow
12/12/2023, 07:39 PM	Microsoft 365	substrate.office.com	Josh_Patriot@M365t2...	
12/12/2023, 07:39 PM	Microsoft 365	login.microsoftonli...	Josh_Patriot@M365t2...	Allow
12/12/2023, 07:39 PM	Microsoft 365	login.microsoftonli...	Josh_Patriot@M365t2...	
12/12/2023, 07:39 PM	Microsoft 365	login.microsoftonli...	Josh_Patriot@M365t2...	
12/12/2023, 07:39 PM	Microsoft 365	login.microsoftonli...	Josh_Patriot@M365t2...	Allow

Created date time ↓	Traffic type	Destination FQDN	User principal name
12/12/2023, 07:39 PM	Private		Josh_Patriot@M365t2...
12/12/2023, 07:39 PM	Private		Josh_Patriot@M365t2...
12/12/2023, 07:38 PM	Private		Josh_Patriot@M365t2...



### Basic info

```
{
  "createdDateTime": "12/12/2023, 07:39 PM",
  "tenantId": "d4ace588-1f7a-4eed-8f7d-c881aaba7036",
  "destinationIp": "192.168.100.164",
  "destinationPort": 3389,
  "destinationFODN": "",
  "sourceIp": [REDACTED],
  "sourcePort": 51589,
  "deviceId": "6bed7cee-e53b-43e2-9a32-1f1bc580857f",
  "deviceOperatingSystem": "Windows 10 Enterprise",
  "deviceOperatingSystemVersion": "10.0.19045",
  "userId": "74bdef0b-a982-4c32-b45c-431b9fed3845",
  "userPrincipalName": "Josh_Patriot@M365t29811314.onmicrosoft.com",
  "networkProtocol": "IPv4",
  "trafficType": "Private",
  "agentVersion": "1.6.51",
  "transactionId": "57f3b421-735d-4a62-8502-74a7ff301793",
  "connectionId": "nAVhvXi+DEiXVzhH.0.0",
  "sessionId": "",
  "client": "Client"
}
```

# Log Fishing

A close-up photograph of a map with several red pushpins. The pushpins are scattered across the map, with one in sharp focus in the foreground and others blurred in the background. The map shows streets and some text, including 'WALCOTT' and 'ROAD'.

# Links

[Aka.ms/ssedeploy](https://aka.ms/ssedeploy)

# Microsoft SSE Licensing

---

## Microsoft Entra Suite

\$12.00 user/month

The Microsoft Entra Suite combines network access, identity protection, governance, and identity verification solutions. A subscription to Microsoft Entra ID P1 or a package that includes Microsoft Entra ID P1 is required.

Special pricing is available for Microsoft Entra ID P2 and Microsoft 365 E5 customers.

[Try for free](#)

[Contact Sales >](#)

## Microsoft Entra Internet Access

\$5.00 user/month

[Try for free](#)

[Contact Sales >](#)

Microsoft Entra Internet Access helps you:

- Secure access to all internet and SaaS applications and resources.
- Extend conditional access policies to the internet.
- Keep your users and devices safe from internet threats.
- Easily manage and monitor your internet access policies for your hybrid workforce through a unified Zero Trust policy engine.

## Microsoft Entra Private Access

\$5.00 user/month

[Try for free](#)

[Contact Sales >](#)

Microsoft Entra Private Access helps you:

- Elevate network access security with a Zero Trust network access (ZTNA) solution.
- Bring adaptive identity security to all your private applications and resources.
- Deliver fast and easy access for users at global scale.

# Entra Suite Licenses - Expanded

**Plans and pricing** [Compare details](#) [Prerequisites](#)

Standard prices are shown below. If your organization qualifies for special pricing, it will be shown at checkout before the final purchase.

Plans	Subscription length & unit price (USD)	Description	Tags <span>?</span>
Microsoft Entra Suite (Trial)	Free for 1 month	Microsoft Entra Suite is an offering that consists of Microsoft Ent...	TRIAL
Microsoft Entra Suite for FLW (Trial)	Free for 1 month	Microsoft Entra Suite is an offering that consists of Microsoft Ent...	TRIAL
Microsoft Entra Suite for FLW	1 month - \$9.60 license/month 1 year - \$8.00 license/month, \$96.00 license/year 3 years - \$8.00 license/month, \$96.00 license/year, \$288.00	Microsoft Entra Suite is an offering that consists of Microsoft Ent...	
Microsoft Entra Suite	1 month - \$14.40 license/month 1 year - \$12.00 license/month, \$144.00 license/year 3 years - \$12.00 license/month, \$144.00 license/year, \$432	Microsoft Entra Suite is an offering that consists of Microsoft Ent...	
Microsoft Entra Suite Add-on for ...	1 month - \$7.20 license/month 1 year - \$6.00 license/month, \$72.00 license/year 3 years - \$6.00 license/month, \$72.00 license/year, \$216.00	Microsoft Entra Suite is an offering that consists of Microsoft Ent...	
Microsoft Entra Suite Add-on for ...	1 month - \$10.80 license/month 1 year - \$9.00 license/month, \$108.00 license/year 3 years - \$9.00 license/month, \$108.00 license/year, \$324.00	Microsoft Entra Suite is an offering that consists of Microsoft Ent...	

# Security Boundaries



Identity



Workstation



Network



The background is a light blue color filled with a repeating pattern of speech bubbles. Each bubble is a different color (red, yellow, pink, white) and contains a dark blue question mark. The bubbles are scattered across the entire frame, creating a dense, textured effect.

# Questions, Comments – Open Forum



