



Azure Active Directory Integration



Revision History

| Sl No. | Version | Date | Author | Description |
|--------|---------|-----------|----------------|----------------------|
| 1 | Draft | 7/12/2023 | Anandakrishnan | Azure AD Integration |

Table of Contents

Contents

| | |
|--|----|
| Revision History | 2 |
| Table of Contents..... | 3 |
| Overview..... | 4 |
| Azure Account Creation General Guidelines..... | 5 |
| cnMaestro Azure Configuration..... | 6 |
| Client Details and Troubleshooting..... | 13 |

Overview

As a component of Microsoft Enterprise, Azure Active Directory (Azure AD) is an enterprise identity service that offers single sign-on, multifactor authentication, and conditional access to protect against 99.9% of cyberattacks.

cnMaestro provides a platform to integrate with Azure AD as an enterprise application to authenticate users. The integration is available in the Guest Access Profile configuration.

This document is applicable only for cnMaestro cloud.

Deployment Model and Use Case

Schools /University

TBD/TBA

Azure Account Creation General Guidelines

1. Ensure that Administrator role and other permissions (global role for managing Azure app) are provided for the user to authorize the azure integration on cnMaestro.

Sample role assigned for an Administrator user below.

+ Add assignments × Remove assignments Refresh | Got feedback?

Administrative roles
Administrative roles can be used to grant access to Azure AD and other Microsoft services. [Learn more](#)

Search by name or description Add filters

| Role | Description | Resource Name | Resource Type | Assignment Path | Type |
|--|---|---------------|---------------|-----------------|----------|
| <input type="checkbox"/> Application Administrator | Can create and manage all aspects of app registrations and enterprise apps. | Directory | Organization | Direct | Built-in |
| <input type="checkbox"/> Global Administrator | Can manage all aspects of Azure AD and Microsoft services that use Azure AD identities. | Directory | Organization | Direct | Built-in |

2. Once the Authorize step is successfully completed, cnMaestro guest portal will onboard this tenant account.
3. Ensure that all the users allowed to login are part of the same Tenant ID. When any user signs in, cnMaestro will check its tenant ID.
4. End users sign-in will happen in two steps.
 - a. Needs to have his AD authorized on cnMaestro.
 - b. The user sign-in happening for right tenant id.

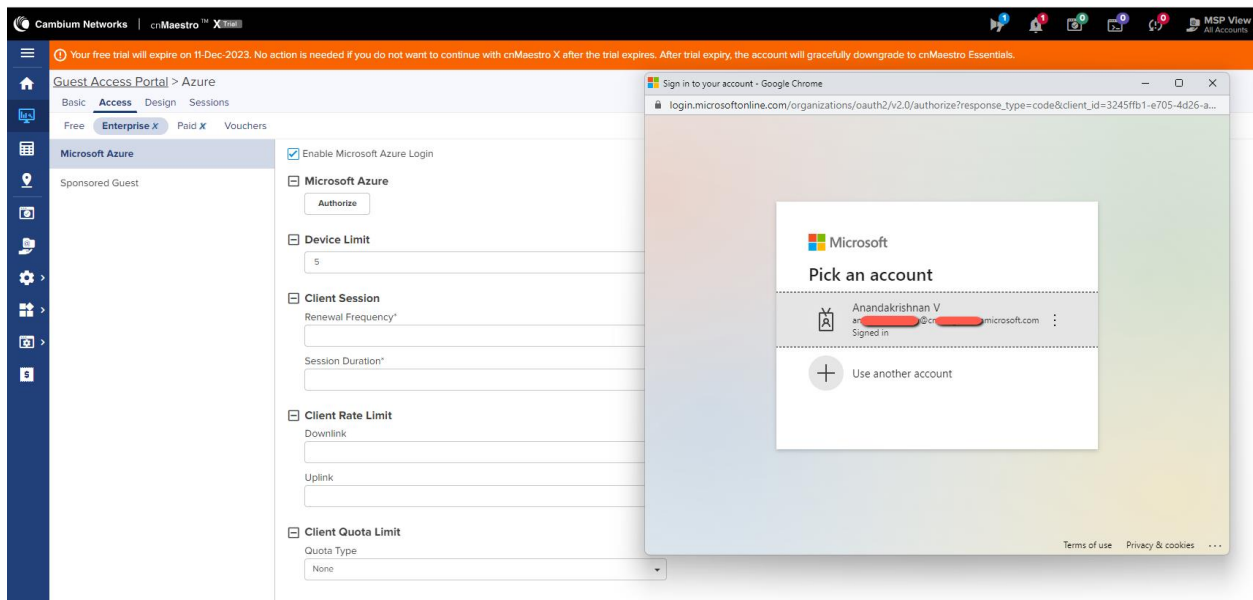
cnMaestro Azure Configuration

Step 1: Create a Guest Access Profile in cnMaestro.

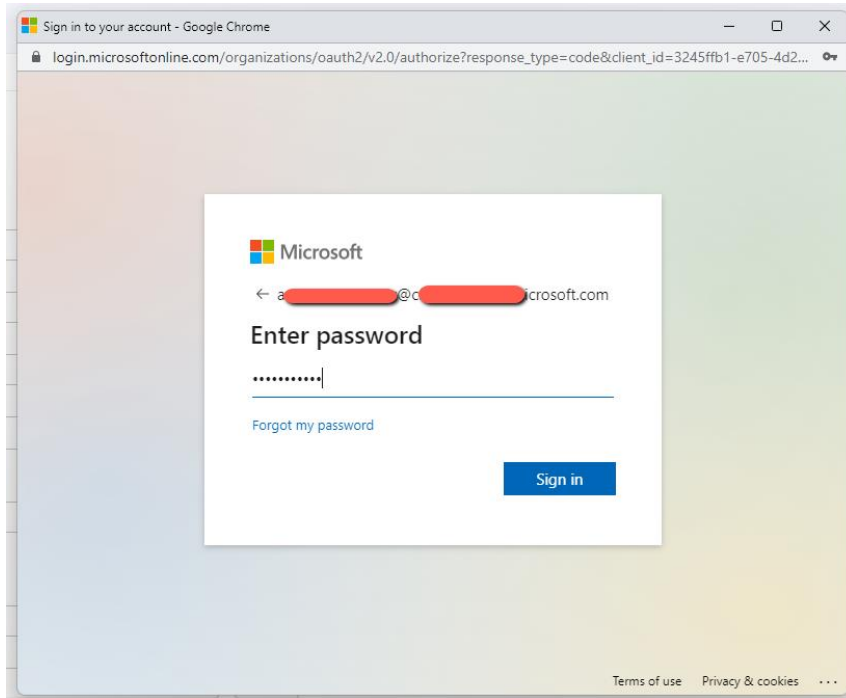
Refer the user guide for Guest Access profile creation.

Step 2: Select Enterprise option and enable Microsoft Azure Login

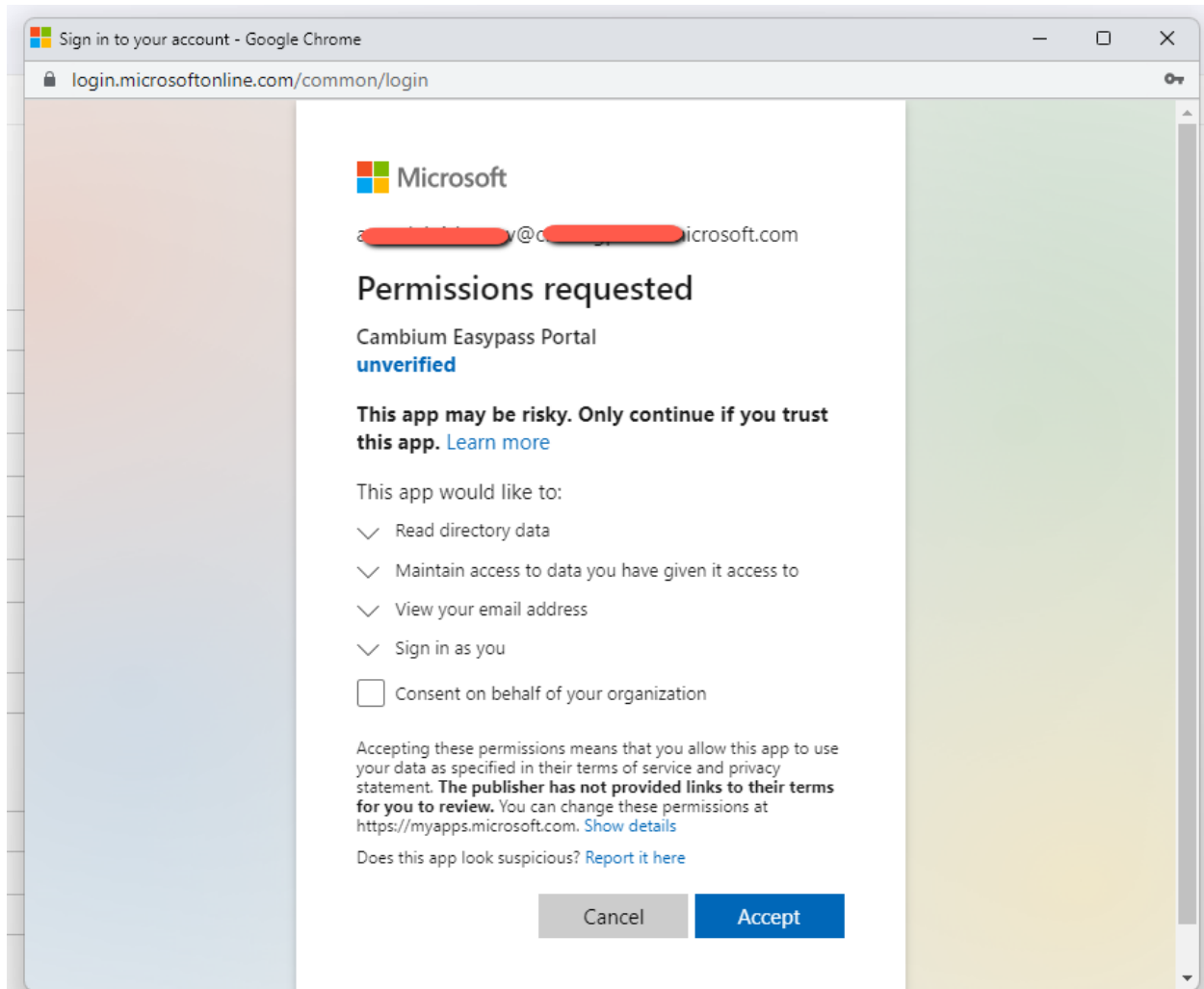
After clicking on Authorize, a pop window will open, login to your azure account (user which has admin rights), if already logged in, select the account to login,



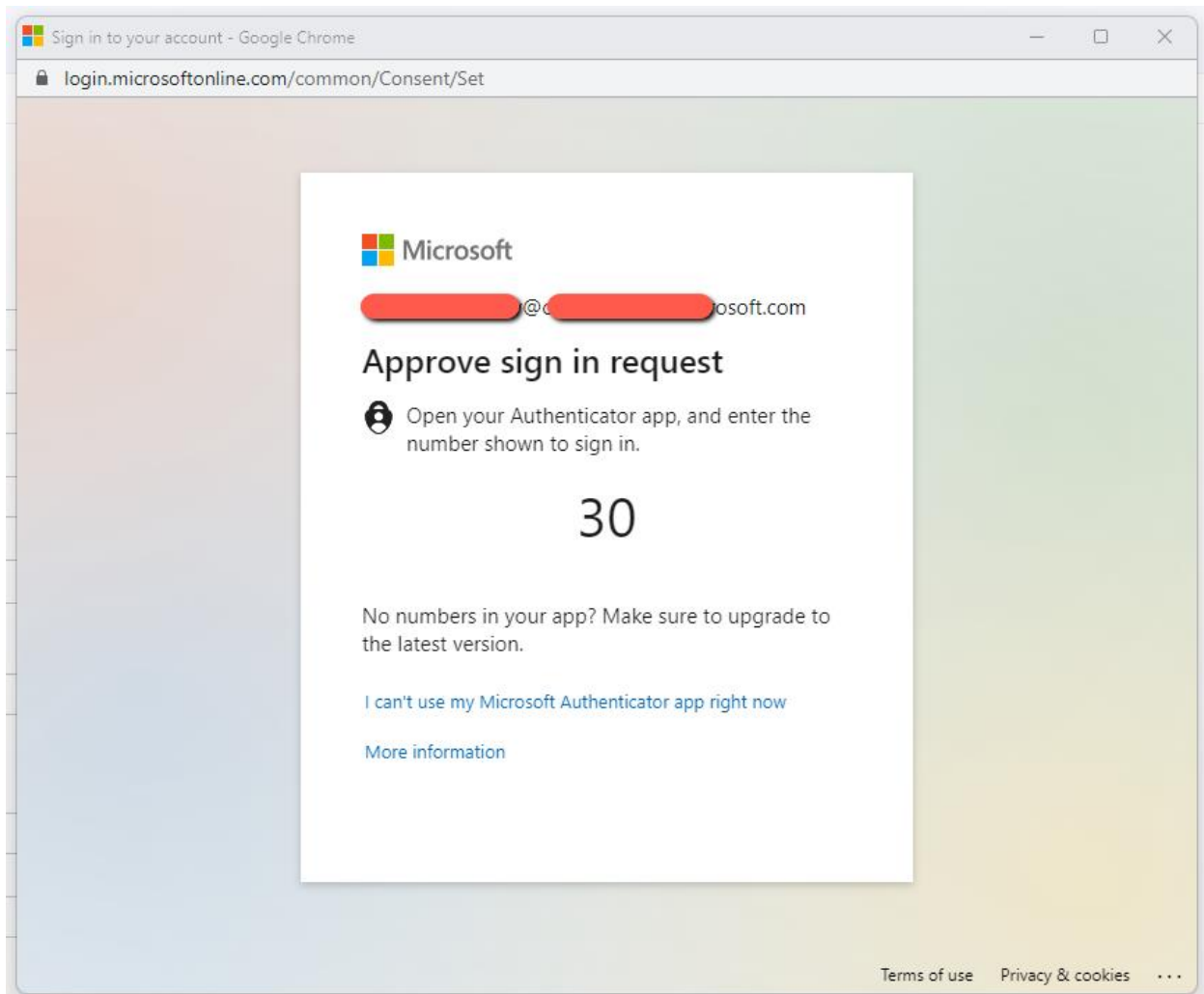
Step 3: Key-in password and click on Sign in



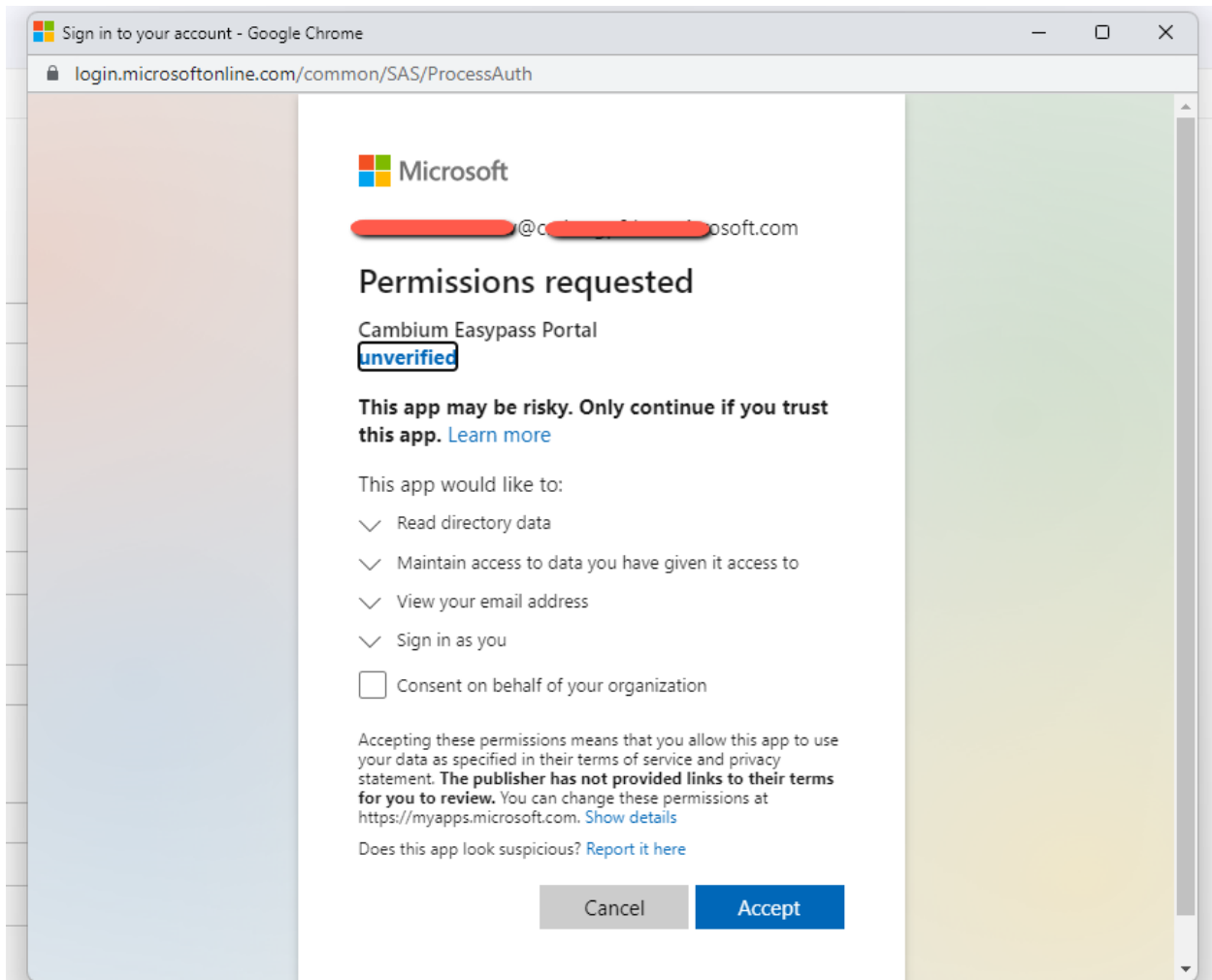
Step 4: Select the check box and Click on Accept



Step 5: If you have MFA enabled, enter the number shown in the logging screen on your phone app to allow sign-in



Step 6: Once the number is entered on the mobile phone sign-in request, the window automatically pops up the accept page, select the check box, and click on the Accept button.



Step 7: Once accept is clicked, authorize step will complete and cnMaestro guest portal will onboard this tenant account. Details of the tenant account will be displayed automatically on cnMaestro. All the allowed groups will be displayed on the allowed groups text box.

Guest Access Portal > Azure

Basic **Access** Design Sessions

Free **Enterprise X** Paid X Vouchers

Microsoft Azure

Sponsored Guest

Enable Microsoft Azure Login

Microsoft Azure

Authorize

Admin Email
[redacted]@[redacted].com

Azure Primary Domain
[redacted].microsoft.com

Allowed Domains
[redacted].microsoft.com

Allowed Groups
Select or Search...

Students
IT Admin
Teachers

Client Session

Renewal Frequency*
5 Min(s) Valid range is 1-2628000 min(s)

Session Duration*
4 Min(s) Valid range is 1-2628000 min(s)

Step 8: Please select the groups to which access needs to be allowed.

Guest Access Portal > Azure

Basic **Access** Design Sessions

Free **Enterprise X** Paid X Vouchers

Microsoft Azure

Sponsored Guest

Enable Microsoft Azure Login


Microsoft Azure

Authorize

Admin Email
[redacted]@microsoft.com

Azure Primary Domain
[redacted]@microsoft.com

Allowed Domains
[redacted]@microsoft.com

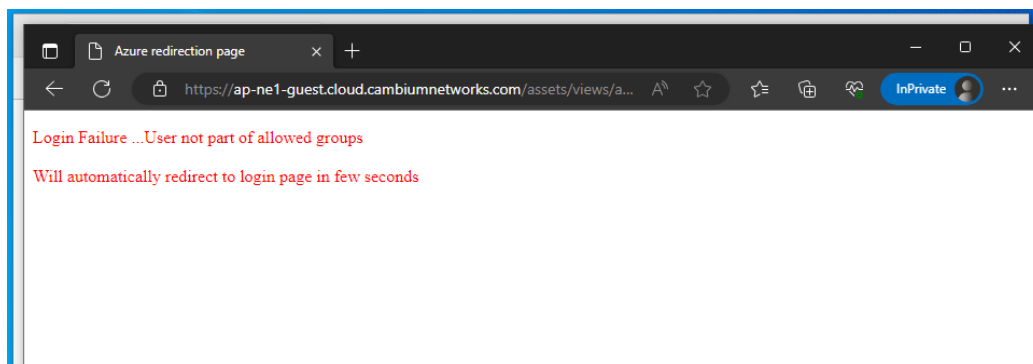
Allowed Groups
Students x  Choose the allowed groups
Select or Search...

Device Limit
5

Client Session
Renewal Frequency*
5
Session Duration*
4

Client Rate Limit

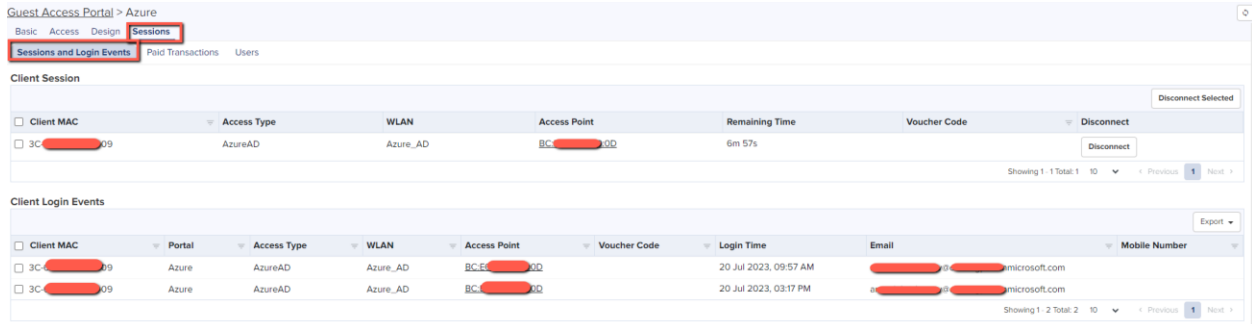
Anyone attempting to log in if they're not a member of the student's group will be denied access.



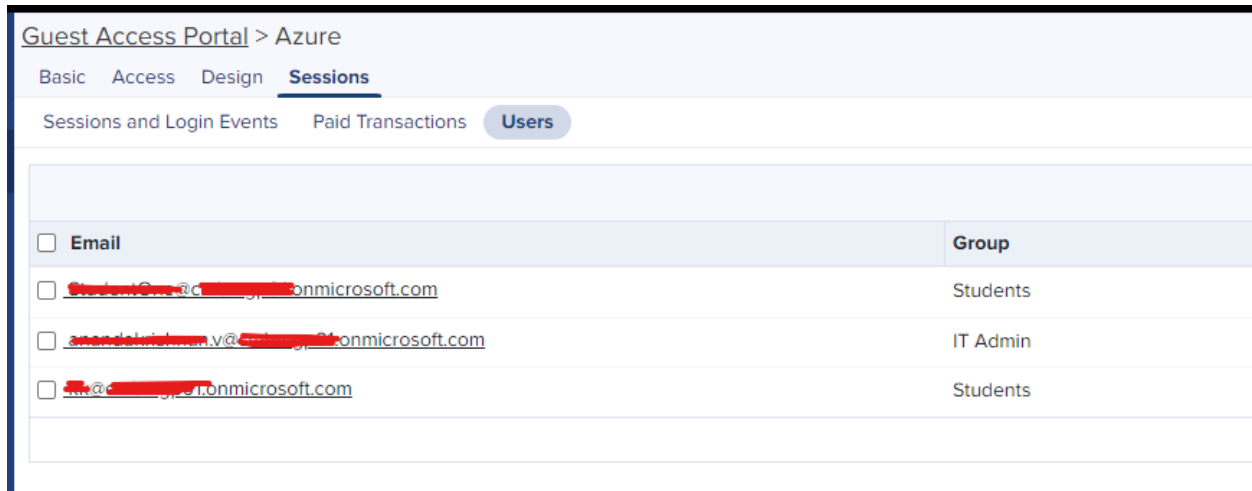
Client Details and Troubleshooting

The user login details can be viewed from the cnMaestro Guest Access Profile, attaching a screenshot from cnMaestro.

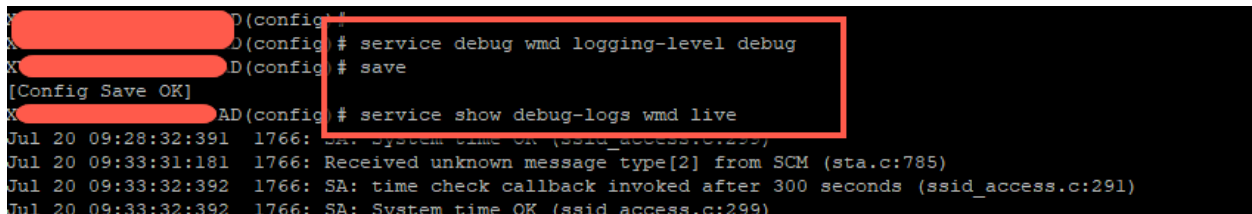
The sessions details tab will display the remaining session time, username, Login time and other details.



The users tab will show the signed in users along with the group details.



The details of the client group returned by Azure will be available in the wmd logs on the AP, to view the logs, enable debug level wmd logging and save the configuration.



Below logs are from AP when client is authenticated, the boxed section will explain the session time and the quota limit configured on the cnMaestro.

```
Jul 20 09:47:32:247 1766: CTRLR: DA sent[208]: {"msgId": 3, "cmac": "[REDACTED]", "status": true, "ssid": "Azure_AD", "up": 2050, "down": 2049, "qType": 0, "qUp": 0, "qDown": 0, "validity": 600, "accessType": 11, "filterId": "IT Admin", "mType": 1}
Jul 20 09:47:32:247 1766: CTRLR: rcvrd msg type[3], total rcvrd reply count[439] (ctrlr.c:1154)
Jul 20 09:47:32:247 1766: CTRLR: Rcvd ga update for client[REDACTED]-[REDACTED] (ctrlr.c:591)
Jul 20 09:47:32:248 1766: CTRLR: WLAN name[Azure AD] found in the controller ga update msg (ctrlr.c:635)
Jul 20 09:47:32:248 1766: CTRLR: Client[REDACTED] on Azure AD allowed sess[600] rl[2050000:2049000] q[0][0:0] (ctrlr.c:665)
Jul 20 09:47:32:248 1766: GA client[REDACTED] ssid[Azure AD] session started for [600] seconds (hotspot.c:794)
Jul 20 09:47:32:248 1766: Hotspot client[REDACTED] on wlan[Azure AD], ga[1], psk[0:0], sess[600], filter[IT Admin] (cache.c:502)
Jul 20 09:47:32:248 1766: Hotspot client[REDACTED] on ssid[Azure AD] no matching filter_id[IT Admin] found in config (cache.c:530)
Jul 20 09:47:32:248 1766: No RADIUS Accounting Server configured for wlan 1 (common.c:126)
Jul 20 09:47:32:248 1766: For client[REDACTED] no RADIUS Server found, skip the RADIUS accounting (session.c:261)
Jul 20 09:47:32:248 1766: GA client[REDACTED] moved from state[Redirected] to new state[Authenticated] (hotspot.c:627)
Jul 20 09:47:32:248 1766: Hotspot client nft[add element ip hotspot allowed-clients { [REDACTED] }] (sta.c:646)
Jul 20 09:47:32:368 1766: Hotspot client nft[add element ip6 hotspot allowed-clients { [REDACTED] }] (sta.c:661)
Jul 20 09:47:32:459 1766: client[REDACTED]: filter[IT Admin], wlan = 1, session_time = 600, user[] (xrp.c:363)
Jul 20 09:47:32:459 1766: XRP[WR]: [REDACTED] dynamic_rate_limit[2050][2049] chain setup (rate_limit.c:437)
Jul 20 09:47:32:459 1766: Client[REDACTED] add rate limit up[2050] down[2049] kbps to netfilter (rate_limit.c:325)
Jul 20 09:47:32:460 1766: Client[REDACTED]
```

On the SAME AP, one can enforce rules based on the group information received from the Azure.

Here a second client is signed in and the filter returned from the Azure AD is “student”

```
Jul 20 10:15:41:011 1766: CTRLR: DA sent[208]: {"msgId": 3, "cmac": "3C-F8-[REDACTED]65", "status": true, "ssid": "Azure_AD", "up": 2050, "down": 2049, "qType": 0, "qUp": 0, "qDown": 0, "validity": 600, "accessType": 11, "filterId": "Students", "mType": 1}
Jul 20 10:15:41:011 1766: CTRLR: rcvrd msg type[3], total rcvrd reply count[449] (ctrlr.c:1154)
Jul 20 10:15:41:011 1766: CTRLR: Rcvd ga update for client[3C-[REDACTED]65]-[3C-[REDACTED]65] (ctrlr.c:591)
Jul 20 10:15:41:011 1766: CTRLR: WLAN name[Azure AD] found in the controller ga update msg (ctrlr.c:635)
Jul 20 10:15:41:011 1766: CTRLR: Client[3C-[REDACTED]65] on Azure AD allowed sess[600] rl[2050000:2049000] q[0][0:0] (ctrlr.c:665)
Jul 20 10:15:41:011 1766: GA client[3C-[REDACTED]65] ssid[Azure AD] session started for [600] seconds (hotspot.c:794)
Jul 20 10:15:41:011 1766: Hotspot client[3C-[REDACTED]65] on wlan[Azure AD], ga[1], psk[0:0], sess[600], filter[Students] (cache.c:502)
```

On the AP, we have a specific filter and group configuration for this filter, to enforce the policy.

```
group 1
radius-id Students
vlan 10
filter-list precedence
!
```

The AP logs showing user is assigned IP address from VLAN 10

```
Jul 20 10:15:46:813 1766: AP-STA-CONNECTED [REDACTED] (../src/ap/sta_info.c:1332)
Jul 20 10:15:46:813 1766: ioctl COPLANE_STATION_FETCH failed (wmd_hostapd.c:4060)
Jul 20 10:15:46:814 1766: [REDACTED] sta->vlan_id=0 sta->is_vlan_updated=0 sta->neighbor_vlan_idx=0 sta->neighbor_vlan_id=0 (wmd_hostapd.c:4155)
Jul 20 10:15:46:814 1766: STA: [REDACTED] client cache based vlan[10] assigned, current vlan[0] (wmd_hostapd.c:4176)
Jul 20 10:15:46:814 1766: The vlan assigned for [REDACTED] is 10 (wmd_hostapd.c:4343)
Jul 20 10:15:46:814 1766: STA: [REDACTED] on WLAN[wlan16:Azure_AD] set VLAN[10] (driver_hostapd.c:530)
Jul 20 10:15:46:818 1766: STA: [REDACTED] on ssid Azure_AD assigned dynamic vlan[10], wlan vlan[1] (wmd_hostapd.c:4347)
Jul 20 10:15:46:818 1766: STA: [REDACTED] successfully added to coplane-2 on wlan16[Azure_AD] (wmd_hostapd.c:4439)
Jul 20 10:15:46:899 1766: HS STA: [REDACTED] ssid[0:Azure_AD] with portal[2], state[Authenticated] (hotspot.c:869)
Jul 20 10:15:46:899 1766: Client: [REDACTED] add rate limit up[2050] down[2049] kbps to netfilter (rate_limit.c:325)
Jul 20 10:15:47:189 1766: client: [REDACTED] hotspot session updated ga allowed[1] to coplane (sta.c:475)
Jul 20 10:15:47:189 1766: Hotspot client nft[add element ip hotspot allowed-clients ( [REDACTED] (sta.c:646)
Jul 20 10:15:47:349 1766: Hotspot client nft[add element ip6 hotspot allowed-clients ( [REDACTED] (sta.c:661)
Jul 20 10:15:47:529 1766: Client client nft[delete element ip hotspot blocked-clients ( [REDACTED] (sta.c:707)
Jul 20 10:15:47:739 1766: n180211: Set STA flags - ifname=wlan16 addr=[REDACTED] total_flags=0x63 flags_or=0x1 flags_and=0xffffffff authorized=1 (../src/drivers/driver_n180211.c:5525)
Jul 20 10:15:47:739 1766: HS Client: [REDACTED] authorized on wlan[Azure_AD] (wmd_hostapd.c:3312)
Jul 20 10:15:47:739 1766: ap_sta_set_authorized: coplane station entry added (../src/ap/sta_info.c:1340)
Jul 20 10:15:47:740 1766: wlan16: STA [REDACTED] MLME: MLME-REASSOCIATE.indication([REDACTED]) (../src/ap/ap_mlme.c:139)
Jul 20 10:15:47:740 1766: wlan16: STA [REDACTED] MLME: MLME-DELETEKEYS.request([REDACTED]) (../src/ap/ap_mlme.c:187)
Jul 20 10:15:47:740 1766: hostapd sta ga[1] acl pending[0] (../src/ap/hostapd.c:3246)
Jul 20 10:15:47:740 1766: IEEE 802.1X: Ignore STA - 802.1X not enabled or forced for WPS (../src/ap/ieee802_1x.c:1361)
Jul 20 10:15:47:740 1766: wlan16: hostapd_new_assoc_sta: reschedule ap_handle_timer timeout for [REDACTED] (300 seconds - ap_max_inactivity) (../src/ap/hostapd.c:3277)
Jul 20 10:15:47:740 1766: n180211: ifindex 11 already in the list (../src/drivers/driver_n180211.c:7162)
Jul 20 10:15:47:740 1766: Client [REDACTED] unauthorized event on wlan16 (wmd_hostapd.c:3695)
Jul 20 10:15:47:741 1766: CTRLR: Received STA [REDACTED] IP[10.10.10.10] update event (ctrl.c:278)
Jul 20 10:15:47:741 1766: GA client [REDACTED] IP[10.10.10.10] updated (wmd_hostapd.c:1742)
Jul 20 10:15:47:741 1766: Client [REDACTED] authorized event on wlan16 (wmd_hostapd.c:3680)
```

The client details on the AP shows clients connected to the same SSID, but in different VLAN.

```
XV2-2-51200D-AzureAD(config)# show wireless clients
MAC          VENDOR  AGE(sec)  MODE  STREAM  SLEEP  RADIO  WLAN  VLAN  802.11-AUTH  NAME          SSID          IPv4
[REDACTED]  -65 Intel    2         an    1       n       2      1    10    y            IN01-LR08TLVK Azure_AD 10.10.10.101
[REDACTED]  -09 Intel   1967     ac    2       n       2      1    1     y            IN01-GRNFQSQ2 Azure_AD 10.110.130.9
Total number of clients: 2
XV2-2-51200D-AzureAD(config)#
```

QnA

How periodically cnMaestro will sync with Azure AD - 24 hrs.