SiteKiosk Online Cloud – Microsoft Entra ID Configuration Guide

These instructions apply only to SiteKiosk Online **Cloud** customers who want to enable Microsoft Entra ID authentication for their SiteKiosk Online teams.

---

1. Custom Subdomain

Each Cloud customer using Entra ID must have a unique subdomain on the SiteKiosk Online Cloud platform.

- You can choose the subdomain name used for your organization.
- The subdomain must only contain alphanumeric characters (letters and numbers, no spaces or special characters).
- Your Cloud URL will have this format:
  `https://<yoursubdomain>.us.sitekiosk.online`
  Example: `https://yourcompany.us.sitekiosk.online`

Note the subdomain and info below and send it to us so we can complete the setup:

1. Subdomain
2. The full Entra ID **User Principal Name (UPN)** of the initial SiteKiosk Online team administrator
   Example: `username@azureaccountname.onmicrosoft.com`
3. The **Entra ID user group name** that contains the users who should be authorized to access the SiteKiosk Online team.
4. The following two values from the Entra Overview page:
   a. **Directory (tenant) ID**
   b. **Application (client) ID**

2. Create the Entra ID App Registration

In your Microsoft Entra ID (Azure portal), create an application for SiteKiosk Online Cloud:

1. Open **App registrations** and click **New registration**.
2. Enter a descriptive **Name.** We will refer to this as “MyEntraAppName” below.
3. At the bottom of the page under **Redirect URI**, enter the Redirect URI with the following pattern:
   `https://<yourSubdomain>.us.sitekiosk.online/SkoIdentityService/si`

`gnin-oidc-<YourEntraAppName>`

- `<yourSubdomain>` is the custom Cloud subdomain you chose.
- `<yourEntraAppName>` is an identifier you choose (letters and numbers only), and will also be used as the configuration name in SiteKiosk Online.

4. Complete the registration.

Note the Entra app name you chose and send it to us along with the other information so we can complete the setup. In this example "YourEntraAppName" was used.

3. Configure Authentication and Logout URL

1. In the Entra ID app you just created, open the **Authentication** section.
2. Under **Redirect URI configuration**, click the "Add Redirect URI" button then select "Web" and enter the URL with this pattern:
   `https://<yourSubdomain>.us.sitekiosk.online/SkoIdentityService/signout-oidc-<yourEntraAppName>`
3. Save your changes.

This ensures that users are correctly logged out of SiteKiosk Online when they sign out from Entra ID.

5. Create a Client Secret

1. In the same Entra ID app, go to **Certificates & secrets**.
2. Click the **New client secret** button.
3. Enter a description and choose an appropriate expiration period.
4. Click **Add**, then copy the **Value** of the client secret immediately and store it securely.

Note the client secret value and send it to us along with the other information so we can complete the setup.

6. Assign Permissions to the Entra ID App

You must grant the app permissions so SiteKiosk Online Cloud can read users and groups from your directory.

1. In the Entra ID app, open the **API permissions** menu.
2. Click the **Add a permission** button.
3. Select **Microsoft Graph**.

4. Choose **Application permissions**.
   Add the following permissions:
   - `Group.Read.All`
   - `User.Read.All`
5. Click **Grant admin consent** and confirm.

All steps to configure this in Entra are now complete. Below is a checklist of information you will need to send to your contact to complete the Entra authentication settings for SiteKiosk Online Cloud.

Checklist of Details needed to complete Entra setup

Send the information below to your contact at SiteKiosk:

1. Subdomain
2. Application (client) ID
3. Directory (tenant) ID
4. Entra app name
5. Client secret value
6. Entra user group name
7. Entra User Principal Name (UPN) for initial administrator. **Example**: `username@azureaccountname.onmicrosoft.com`

Working With Teams After Entra ID Activation

- The Entra ID user you selected as the team administrator should log in via the SiteKiosk Online Cloud login page at your custom subdomain, example: https://yourcompany.us.sitekiosk.online.
- Once logged in, the administrator can:
  - Manage team rights and permissions for other Entra ID users and groups.
  - Add or remove Entra ID groups from the team configuration.
- If Entra ID authentication is later disabled for a team, Entra ID users will lose access to that team, and you may need to reconfigure local users if desired.
- After activating Entra ID authentication, any users you have created through the SiteKiosk Online interface will be removed.