SiteKiosk Online Server (On-Premise) – Microsoft Entra ID Authentication

These instructions apply only to self-hosted / on-premise SiteKiosk Online Server customers who want to authenticate users via Microsoft Entra ID.

1. Prepare Microsoft Entra ID

After logging in to Entra, note these values from the Entra overview page. You will need to add them to the SiteKiosk Online Server settings later.

- **Application (client) ID**
- **Directory (tenant) ID**

1.1 Create the app registration

1. Open **App registrations** and click **New registration**.
2. Enter a descriptive **Name.** We will refer to this as “YourEntraAppName” below.
3. At the bottom of the page under **Redirect URI**, select Web from the platform drop down and enter the Redirect URI with the following pattern:
   `https://<yourHostName>/SkoIdentityService/signin-oidc-<YourEntraAppName>`
   - `<yourHostName>` is the hostname for your self-hosted instance.
   - `<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 app registration.

1.2 Add redirect and logout URIs

Use the **public hostname** of your on-premise SiteKiosk Online Server in the URLs where you see .

1. In the Entra app, open **Authentication**.
2. Add a **Logout URI** in this format:
   `https://<yourHostName>/auth/signout-callback-oidc-<yourEntraAppName>`
3. Save your changes.

1.3 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 and store it securely.
5. Take note of the client secret value. You will need it later.

1.4 Assign required permissions

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 complete the Entra authentication settings in the backend SiteKiosk Online Server settings.

Checklist of Details needed to complete Entra setup

You will need the following details to add Entra authentication to your SiteKiosk Online Server.

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

---

2. Configure Entra in SiteKiosk Online Server

The following steps describe the procedure to activate Entra authentication in the backend SiteKiosk Online settings. You can access this on your server with the Windows admin credentials you designated during the SiteKiosk Online installation. (e.g. https://<*yourhostname.com*>/administration). You will need the details that you noted in the steps above.

2.1 Open the SiteKiosk Online server administration

1. Open a browser and go to the administration URL of your **on-premise SiteKiosk Online Server**. (e.g. https://<*yourhostname.com*>/administration)
2. Log in with your **Windows administrator** credentials.

2.2 Open external authentication provider settings

1. In the top menu, click **Settings**.
2. Then click the **Edit Configuration** link under **External Authentication Provider Settings**.

2.3 Add the Entra ID domain configuration

1. Under **Configured Entra ID Domains**, click **Add New**.
2. Fill in the form with the values from your Entra app:
   - **Application name** (the app name from Entra, e.g. `SiteKioskOnline`)
   - **Directory (tenant) ID**
   - **Application (client) ID**
   - **Client Secret Value**
3. Click **Test** to verify the connection.
4. When the test is successful, click the **green Save button** and wait until the configuration is stored and listed under configured Entra ID domains.

If you do not click **Save**, the settings are not kept even if the test was successful.

3. Assign Entra Authentication to a Team

3.1 Use an existing team or create a team

1. In the administration menu, click **Teams**.

2. If no team exists, click **New Team**, fill in the required fields, and create one.

You must have at least one team before assigning Entra authentication.

3.2 Activate external authentication for a team

1. On the Teams page, find the team you want to connect to Entra.
2. In the **External Authentication** column, click **Activate External Authentication** (or the “not configured” link).
3. In the configuration dialog:
    - Select your **Entra provider** (the configuration name you added under Settings).
    - Enter the **Entra group name** that contains the users who should access this team.
      Enter the **username** of the team administrator. **Example**:
      `username@azureaccountname.onmicrosoft.com`
4. Click **Test**:
    - If the test fails, double-check that you are using the **Entra group name** (security group that holds your users), not the app registration name.
5. When the test succeeds, click **Activate**.
6. Confirm the warning that existing manually created users may be removed and replaced by users from the Entra group.

After activation, the Teams page will show options to **Modify** or **Deactivate** external authentication, indicating Entra is active for that team.

4. Test Entra Login

1. Log out of the SiteKiosk Online Server administration backend.
2. On the login page, choose the appropriate **Authentication provider**. This will be displayed as the registered app name in Entra.
3. Click **Sign In with Microsoft**.
4. If prompted, select the **team** you want to log in to.
5. In the Microsoft sign-in window:
    - Select an Entra user account that belongs to the configured group.
    - Enter the user’s password.
    - Complete **MFA / 2FA** if required.
6. After successful sign-in, you are logged into the selected team with your Entra user.

5. Verify Entra Users and Groups in SiteKiosk Online Server

1. Under the Users menu, go to the **User groups** tab.
2. Confirm that a user group corresponding to your Entra group now exists and that the Entra users from that group are listed.
3. As an administrator, assign appropriate **roles/permissions** to the Entra user or group so they can log in and use the team as intended. This step is required for these users to have SiteKiosk Online user role permission to be able to log in.

With these steps, Microsoft Entra ID authentication is fully enabled for your **on-premise SiteKiosk Online Server**, allowing your Entra users to log in securely with their Microsoft accounts.

Working With Teams After Entra ID Activation

- 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.