

SSO

Azure SAML Single Sign On

The following documentation is for Kiyocrm Version 7.x; to see documentation on the same topic for Version 8+

Azure SAML Single Sign On

Kiyocrm can utilize a third-party identity provider such as Microsoft Azure Active Directory and the SAML protocol to achieve single sign-on authentication. You can then use Azure AD to control who has access to Kiyocrm and enable automatic sign in.

Considerations

- We recommend using the latest release of Kiyocrm 7.x to benefit from the latest improvements and fixes.
- The user must exist in both Azure AD and Kiyocrm for login to be successful.
- The usernames in Kiyocrm 7.x must match the email address in Azure. If you have used abbreviated or shortened usernames these should be changed to email addresses in advance.

1. Setup APP in Azure

The first step is to create a new Enterprise Application in Azure. This app defines how Azure, as the Identify provider (IdP) will interact with your Kiyocrm instance. Doing so will also provide you with the required values and certificate to configure Kiyocrm. SAML apps in Azure are unique to each instance, as the CRM URL is verified as part of the sign in process. If SAML is needed for multiple staging, test or production environments a new app will be needed for each.

1.1. Create the new application

Login to Microsoft Azure and navigate to 'Azure Active Directory' section using the icon on the home page

From the left-hand Menu select 'Enterprise applications'

[SuiteCRM SSO Azure side menu](#)

From the top menu, select 'New Application'

[SuiteCRM SSO Azure top menu](#)

From the top menu, select 'Create your own application'

A new side window will open; you can use this to create your application.

1. Enter a descriptive name such as KiyoCRM SAML Authentication'
2. Choose 'Integrate any other application you don't find in the gallery (non-gallery)'
3. Click Create and you will be taken to the 'Application Overview' after a short delay

[Screenshot 9.png](#)

1.2. Configure the new application

From the left-hand Menu select 'Single sign-on' from the Manage category

[SuiteCRM SSO Azure Application side menu](#)

Select SAML from the available options

[SuiteCRM SSO Azure Application protocol select](#)

Click on the pen icon to Edit the Basic SAML Configuration

[SuiteCRM SSO Azure Application SAML configuration](#)

KiyoCRM uses the same value for Entity ID, ACS URL and Sign On URL.

The value should be your KiyoCRM URL in the following format:

{CRM URL}/index.php?action=Login&module=Users

For example: <https://kiyocrmdemo.com/index.php?action=Login&module=Users>

1. In the Identifier (Entity ID) section, enter your KiyocRM URL as prepared in the previous step
2. In the Reply URL (Assertion Consumer Service URL) section, enter your KiyocRM URL as prepared in the previous step
3. In the Sign on URL (Optional) section, enter your KiyocRM URL as prepared in the previous step
4. Verify that the same URL is present in all three of these fields, then click Save

1.3. Store the required settings for later use

Scroll down to the SAML Certificates section and download the Certificate (Base64) and store it for later

Scroll further down and store the Login URL and Logout URL and again, store these for later.

[SuiteCRM SSO Azure Application SAML settings](#)

2. Add users to APP in Azure

Before your users can login to KiyocRM using SSO with Azure, they must be added to the newly created application. Users can be added individually or in groups, depending upon how your Azure Active Directory is configured. Only users which have been added to the KiyocRM SAML Authentication' Application will be able to login.

From within your newly created Enterprise Application:

1. From the left-hand menu, select 'Users and Groups'

[SuiteCRM SSO Azure Application Users and Groups](#)

1. From the top menu, select 'add user/group'

You can now assign either users or groups to your KiyocRM SAML Authentication' Application.

3. Setup SAML in KiyocRM

Before you can finish setting up your users in KiyoCRM you must first enable SAML. Once this step is complete your users will no longer be able to login in the normal way and SSO must be used.

3.1. Enable SAML

Sign in to KiyoCRM as an administrator

Go to Admin → Password Management

[SuiteCRM SSO Enable SAML](#)

Select Enable SAML Authentication

In the SAML Authentication section, add the following information

1. Login URL: Paste the value of the Login URL retrieved from Azure
2. SLO URL: Paste the value of the Logout URL retrieved from Azure
3. X.509 Certificate: Paste the contents of the Base64 Certificate retrieved from Azure

Save your changes

3.2. Enable SAML for your users

Once KiyoCRM has been configured to use SAML, you can configure your individual users to use SAML to login. You must complete this step for each user who will login using SSO.

1. Create or edit an existing CRM User, setting their username to match the email address in Azure.
2. Enable SAML Login for that user, by navigating to the Advanced tab, and checking the SAML2Authenticate
3. You may wish to setup and assign any Roles, Security Groups required for the user at this stage before they first login

[SuiteCRM SSO Users enable SAML](#)

Revision #2

Created 22 May 2025 05:32:37 by Admin

Updated 22 May 2025 10:45:56 by Admin