SAML SSO SETUP

MAXIMIZER™CRM

Contents

Configure SAML based single sign-on (SSO)

Maximizer CRM can act as a SAML2 Service Provider (SP) that will rely on a configured Identity Provider (IDP) for managing user authentication in place of the User Id and password authentication built into the product.

Before you configure SAML settings for SSO into Maximizer, you should have the following ready:
- An Identity Provider
- A public IP address – If you deploy SAML SSO in an on premise environment, your site needs to be visible on the Internet so the IDP can communicate with it.
- An SSL certificate - Your site should be using SSL for its traffic as it is a requirement when using an IDP.
- A certificate for running Maximizer as a service - The SHA256 SSL certificate that needs to be entered into the Request Signing Certificate field when you set up the IDP in Maximizer.
- Each Maximizer user should have an unique email address

Please note:

Maximizer's SSO capabilities use SAML 2.0 standards which are supported by most major Identity Providers. Configuring Maximizer to use SSO requires knowledge of the third-party Identity Provider being used, security certificates, and other system administrator type skills. If you are unsure of how to gain the required configuration information, please refer to your systems administrator, third party Identity Provider documentation, or other content readily available online. Maximizer will not provide any third-party identity provider support.

Gather information from your IDP

Gather the following information from your IDP before configuring Maximizer for SAML SSO.
- The unique identifier of the IDP
- An authentication certificate.

Add an IDP in Maximizer

To add an IDP into Maximizer, go to Maximizer Web Access > Icon Bar > Administration > Settings > Single Sign-on and click **Add Identity Provider** button.

Populate the following fields:

Identity Provider Entity ID	A unique URL that identifies your IDP; obtain the URL from the IDP.
Identity Provider Name	A friendly name for the IDP. The name will be displayed in the login button for the IDP. The length of the name is limited to 32 characters.
Identity Provider Certificate	The authentication certificate issued by the IDP. Obtain the certificate from the IDP.
Identity Provider URL	The URL where Maximizer sends a SAML request to start the login process.
Identity Provider Logout URL	The URL to direct the users to when they click the Logout button in Maximizer. Logout URL is optional. If no Logout URL is entered, the users will see the default logout page provided by Maximizer.
HTTP Binding Type	Select HTTP-POST

Service Provider Entity ID	**On-premise:** This field will be populated automatically. The format of the URL looks like: https://[Your Server]/MaximizerWebAuthentication/SAML2/[Database Name] **CRM Live:** You need to manually enter the URL of your CRM Live site in following format: https://[Your datacenter URL]/SAML2/[Your Account Name] For example: https://caw.maximizercrmlive.com/SAML2/maximizerPMteam
Request Signing Certificate	The certificate must be created and signed with the supported signing algorithm. In this release, only SHA 256 is supported. The certificate needs to be converted to a base64 string. You can save the certificate in a text file. Copy and paste the certificate from the text file into this field.
Signing Algorithm	Select SHA 256
Assertion	Match the Maximizer users with users in IDP; Select Maximizer user ID or email address.
Claim	The default value of the Claim field will be populated automatically based on the assertion. If you select Maximizer User ID in Assertion field, the value for the Claim field will be set to "uid". If you select Email in Assertion field, the value for the Claim field will be set to "mail". The default values do not always match the Claims in IPD. There are two ways to match the values from the two sides: 1. If your IDP allows custom Claims. You can create a custom Claim "mail" in IDP to match the Assertion setting "Email" in Maximizer. 2. If your IDP does not support custom Claims, you need to change the value in the Claim field to match the Claim in IDP.
Service Provider Metadata URL	This is a read only field. It is blank by default. After you create the IDP and open the dialog again, this field will be populated. You need to use this URL when you add Maximizer as a Service Provider in your IDP. Click the copy button to copy the URL to the clipboard.

Note:
Except for the Identity Provider Logout URL field, all the other fields are mandatory.

Enter the values into all the required fields and click **SAVE** button.

Your IDP will be displayed in the SSO screen. In this release, you can only add one identity provider. You can have both Maximizer login and your IDP login turned on. Or you can turn off Maximizer login and only use your IDP.

Before you turn off Maximizer login, you MUST make sure that your users can login using the Identity Provider. If you turn off Maximizer login and you have a problem logging in using your IDP, you will not be able to log in to Maximizer.

Configure the IDP to add Maximizer as a service provider

If your IDP allows uploading Service Provider metadata, upload the Maximizer Service Provider metadata.

Go to Settings > Single Sign-on and open the settings of the IDP by clicking the round button and clicking **Edit**.

Copy the value from the Service Provider Metadata URL field and paste it into your IDP. Use the copy button besides the field to copy the URL to clipboard.

If the IDP requires a file for metadata rather than a URL, the XML can be retrieved manually and saved to an XML file with UTF-8 encoding.

Test login using IDP

Once you have set up your IDP, you can test logging into Maximizer using the IDP in Web Access, Mobile Access, Outlook add-in and Mobile app.

Web Access

When both Maximizer login and custom IDP are enabled in the selected database. The user can log in using Maximizer user ID and password or the custom IDP.

Clicking the IDP login button will go to the IDP login page. After logging in, you will get into Maximizer.

If the selected database does not have a custom IDP, only Maximizer login will be available. Use Maximizer user id and password to login.

After you log in to Maximizer successfully using your IDP, you can turn off Maximizer login. The fields for Maximizer user ID and password in the login page will be disabled. Click the IDP login button to login.

Note
If there is only one database in the server and only custom IDP is enabled in that database, when you try to access the Maximizer Login page, you will be automatically redirected to the Login page of the IDP.
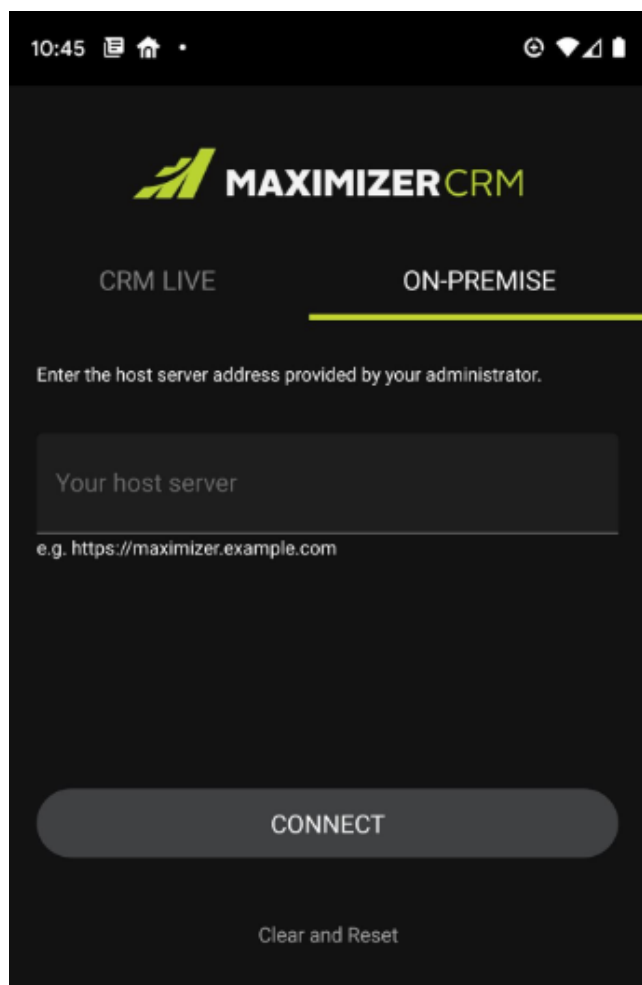
Mobile Access

The login process in Mobile Access works the same way as it does in Web Access. If the selected site has an IDP enabled, the login button for the IDP will be available.

Mobile App

To access Address Books in an on premise environment, you need to enter the URL of the host server. For example, https://maximizer_example.com. Note that, you do not need to enter "/MaximizerWebAccess" in the URL. Tap the Connect button, you will be re-directed to the OAuth login page. Tap "Log in to" field and select an Address Book, the login controls will be displayed based on the enabled IDP in the Address Book.
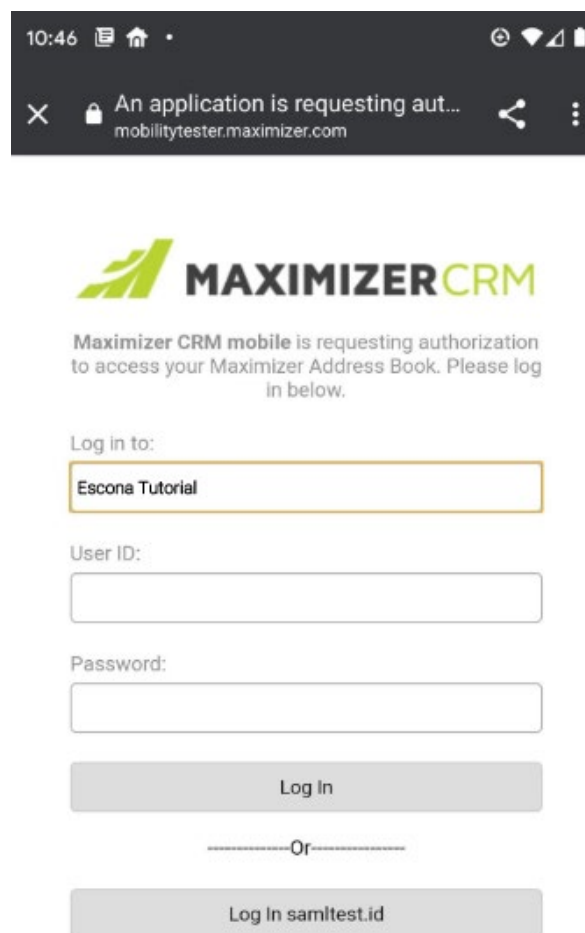
In CRM Live, you need to enter your email address to login. If you have only one CRM Live account, you will be re-directed to the OAuth page with your account name displayed in the login page. If you have multiple accounts, you will need to select an account and then go to the OAuth page to login.

CRM Live

You CRM Live site works the same way as it does in an on premise environment. If you turn off Maximizer login in your site, when you try to access the CRM Live login page, you will be automatically re-directed to the IDP login page. You will not see the Maximizer Login page.

Outlook Add-In

The Outlook Add-in will only allow users to authenticate to a Maximizer account using OAuth workflow, provided that the user's Maximizer account is 2021 R1 and the latest Outlook build has been installed. If a Maximizer account has been setup with a SAML IDP, the Outlook Add-in will allow the user to login through their configured IDP.

Enter the URL of the Maximizer site into Preferences in Outlook Add-In

Clicking the OK button will cause the OAuth dialog to open. If the site has a custom IDP enabled, the Login button for the IDP will be available.

Note
Logging in through OAuth is also available in the Wizards for Outlook add-in.

Windows Administrator and Customization Suite

SAML SSO for logging in to Windows Administrator and Customization Suite is not supported. You can always log in to Windows Administrator and Customization Suite using Maximizer login credential.

Frequently Asked Questions

How to create a certificate?

The certificate generated for Maximizer cannot be a wildcard one, as they are not supported in some IDPs such as Azure AD. Here is an example of creating a certificate using OpenSSL. OpenSSL is free and using the technique guarantees success. With OpenSSL installed, a certificate valid for SHA256 signing can be generated with the follow commands:

openssl req -x509 -nodes -sha256 -days 3650 -newkey rsa:2048 -keyout MaximizerSP_openSSL.pem -out MaximizerSP_openSSL.cer
openssl pkcs12 -export -nodes -out MaximizerSP_openSSL.pfx -inkey MaximizerSP_openSSL.pem -in MaximizerSP_openSSL.cer -passout pass:

How to use Windows PowerShell commands to convert a certificate to base64 string?

You need to create a certificate valid for SHA256. Run the following script:
$fileContentBytes = get-content 'P:\\<Your certificate>.pfx' -Encoding Byte

[System.Convert]::ToBase64String($fileContentBytes) | Out-File 'pfx-encoded-bytes.txt'

Use the text inside the **pfx-encoded-bytes.txt** file as the **Request Signing Certificate.** The certificate needs to be entered into Maximizer SSO settings screen.

How to deal with "access denied" message?

You have set up SAML SSO and try to log in using your IDP. If you encounter the message "access_denied: Access is not possible at this time. Please contact the site administrator", most likely it is caused by an invalid certificate. Follow the steps mentioned above to ensure your certificate is valid.

How to enter a certificate?

When entering a certificate, make sure to remove the start and end tags (---BEGIN CERTIFICATE---, ---END CERTIFICATE---).

Identity Provider Certificate

----BEGIN CERTIFICATE---- MIIDBTCCAe2gAwIBAgIQN33ROaIJ6bJBWDCxtmJEbjANBgkqhkiG9w0BAQsFADAtM

Can I set up Azure Active Directory as an IDP?

Yes. You can set up Azure AD as an IDP to log in to Maximizer. Here is a document for your reference. Please note that **MAXIMIZER**CRM does not provide any support of setting up Azure AD.

MAXIMIZERCRM

Experience MAXIMIZER™CRM

MAXIMIZER™CRM helps small and medium-sized teams consistently overachieve their business goals with centralized, easy-to-use and powerful views of their business data – all in one tab.

Contact Us