

Configure Dmarcian for Single Sign-On

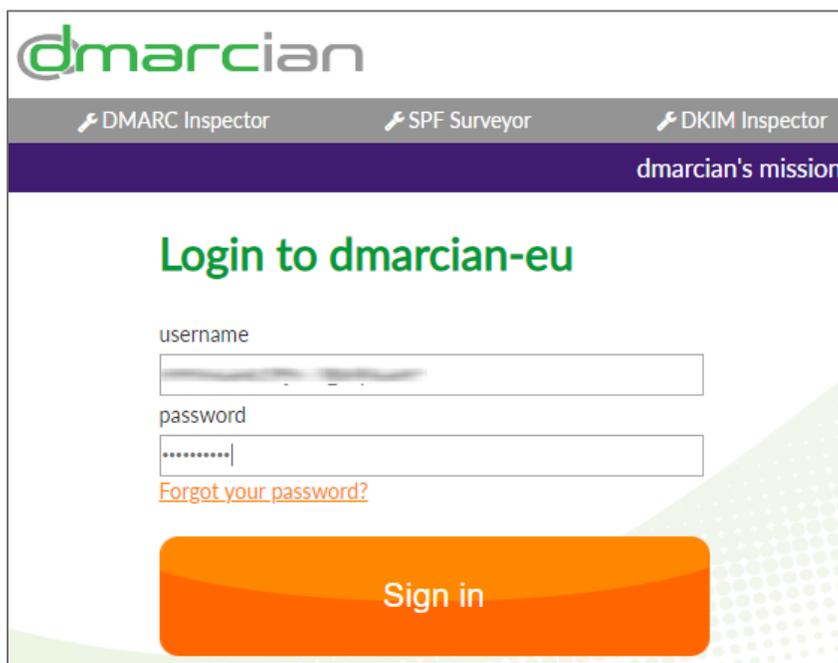
Configuring Dmarcian for single sign-on (SSO) enables administrators to manage users of Citrix ADC. Users can securely log on to Dmarcian by using the enterprise credentials.

Prerequisite

Browser Requirements: Internet Explorer 11 and above

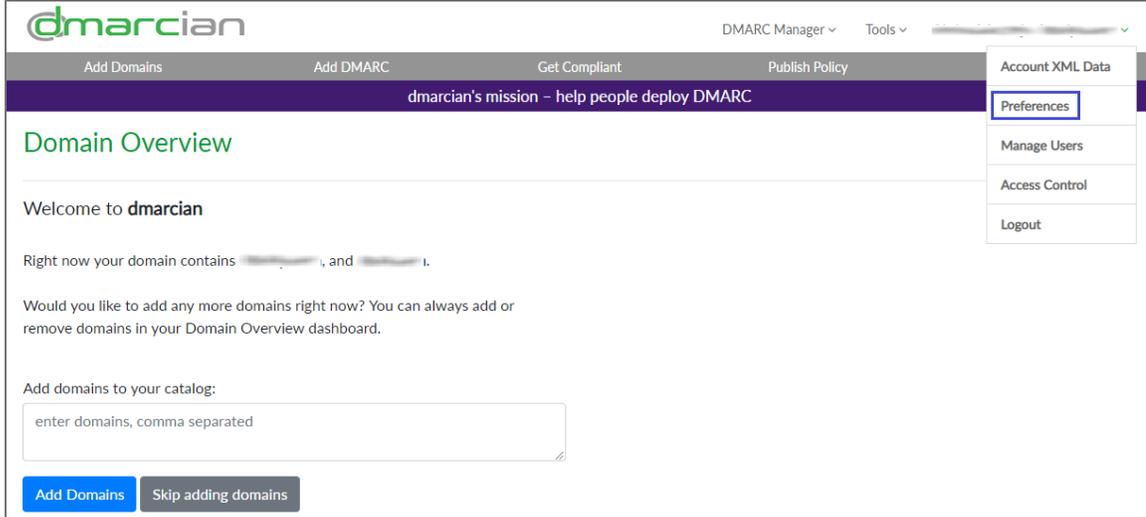
To configure Dmarcian for SSO by using SAML:

1. In a browser, type <https://dmarcian.com/login/> and press **Enter**.
2. Type your Dmarcian admin account credentials (**username** and **password**) and click **Sign in**.

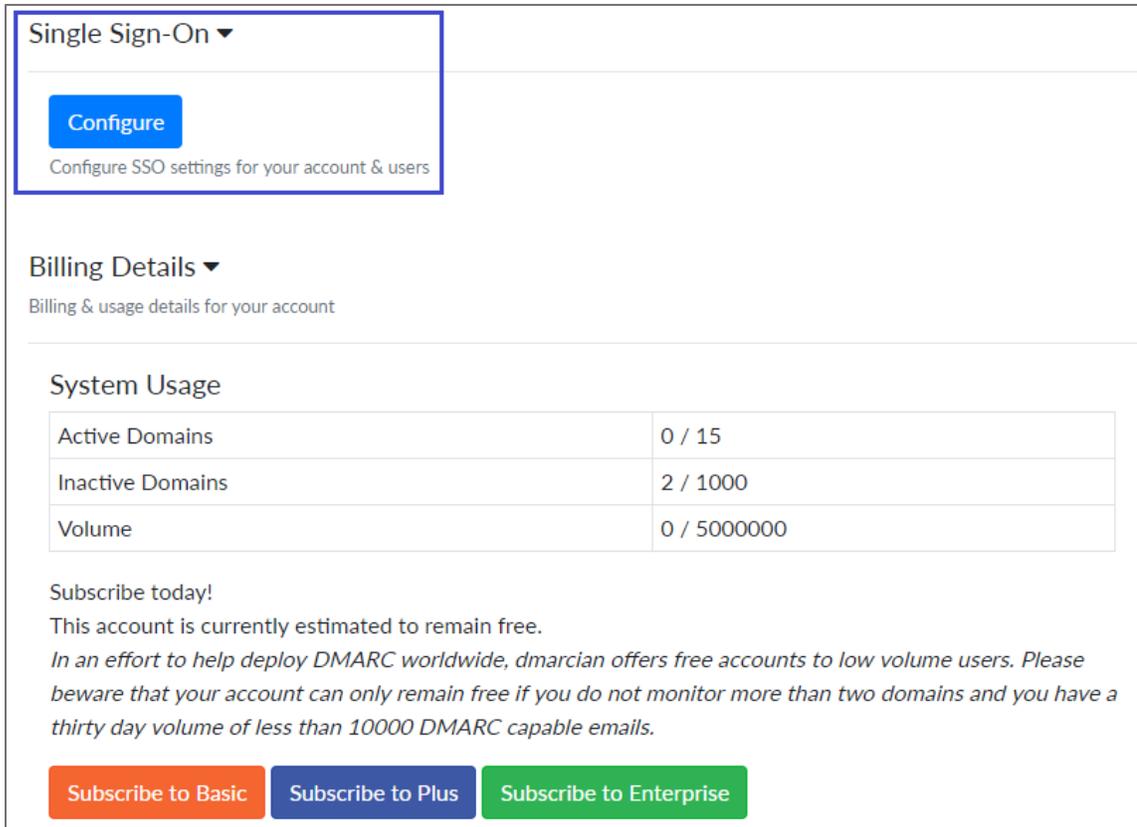


The screenshot shows the Dmarcian login interface. At the top, there is a navigation bar with the Dmarcian logo and three menu items: DMARC Inspector, SPF Surveyor, and DKIM Inspector. Below this is a purple header with the text "dmarcian's mission". The main content area is titled "Login to dmarcian-eu" in green. It contains a "username" field, a "password" field with masked characters, and a "Forgot your password?" link. A large orange "Sign in" button is positioned at the bottom of the form.

3. In the top-right corner, click the user name and select **Preferences** from the list.



4. In the **Preferences** page, scroll down and click **Single Sign-On > Configure**.



5. Enter the values for the following fields:

Field Name	Description
Identity Provider Metadata	Copy and paste the metadata URL or upload the metadata file in XML format. Note: The metadata URL is provided by Citrix: https://ssb4.mgmt.netscalergatewaydev.net/idp/saml/templatedetst/idp_metadata.xml
Attribute Statements	Email address
Login URL	IdP logon URL

SAML Single Sign-On

SAML-based single sign-on (SSO) allows users to authenticate into dmarcian via credentials configured in an identity provider (IDP) of your choice.

Status Enabled Disabled

1. Add dmarcian to your Identity Provider

Copy the below URLs to your IDP to define dmarcian as a service provider.

Assertion Consumer Service URL <https://dmarcian-eu.com/login/ /handle/> Copy
Also known as single sign-on URL - the location where the SAML assertion is sent with an HTTP POST request

Entity ID <https://dmarcian-eu.com/sso/saml/ /sp.xml> Copy
Contains an XML file that describes dmarcian as a service provider

2. Set up Authentication

After you have added dmarcian to your IDP, they will provide you with the following information.

Identity Provider Metadata You have already provided valid metadata. View XML Update

Attribute Statements Email Email
Set the Email attribute as defined in your IDP

3. Set up Login URL

Here is your login URL, you can customize it if you'd like.

Login URL <https://dmarcian-eu.com/login/>
This is the URL users from your company will use to login

Back to Preferences Save

6. Finally, click **Save**.