Configure IBM MaaS360 for Single Sign-On

Configuring IBM MaaS360 for single sign-on (SSO) enables administrators to manage users of Citrix ADC. Users can securely log on to IBM MaaS360 by using the enterprise credentials.

Prerequisite

Browser Requirements: Internet Explorer 11 and above

To configure IBM MaaS360 for SSO by using SAML:

- 1. In a browser, type <u>https://login.maas360.com/</u> and press **Enter**.
- 2. Type your IBM MaaS360 admin account email address and click **Continue**.

Log in to IBM MaaS360		
Continue		
Remember Me Forgot Username or Password?		

3. Type your IBM MaaS360 admin account password and click **Log in**.

Log in to IBM	
Logging in as	Not you?
Password	Forgot password?
•••••	Ø
🗌 Remember me (i	
Log in	

4. In the dashboard page, click **SETUP** > **Settings**.

IBM MaaS360 With Watson	1	Search for Devices, Users or Apps		Q	? 🗕 🖒
HOME DEVICES USERS SECURITY	APPS REPORTS	SETUP			
		Services & Settings	Portal Administration		
My Alert Center		Services	Administrators) 🧿		
Last Analyzed: Monday, April 22, 2019 5:57:57 AM UTC		Settings	Roles		
0 Recently Added	0 No Passcode	Branding	Administrator Logins Report	~	
		Enterprise Integration		My Activity Feed Show All	~
O Out of Compliance	0 Roaming	Cloud Extender		Last Updated On: Friday, April 19, 2019 10:30:00 /	AM UTC
		Azure Integration		Policy Published: Default Android MDM	Policy
Cong Inactivity Policy Published: Default Windo Policy Published: Default Windo			Policy Published: Default Windows MDN	A Policy	
				Policy Published: Default IOS MDM Poli	су
My Advisor 👸 With With		🥝 All	✓ Last 180 Days ✓ Ĉ 🖲	New App: IBM MaaS360	
No Insights Available					

5. In the **Settings** page, click **Administration Settings** > **Advanced** from the left pane.

Settings	Save
Device Enrollment Settings	Login Settings
User Settings	Use this section to configure strong portal authentication for your Administrators.
App Settings	Configure Strong Authentication
Administrator Settings	
🔅 Basic	
C Advanced	

6. Select the **Configure Federated Single Sign-on** check box and click the **Use SAML for Single Sign-on** radio button.

Settings	Save	
Device Enrollment Settings	Login Settings	
● User Settings	Use this section to configure strong portal authentication for your Administrators.	
App Settings	Use SAML for Single Sign-on	
Administrator Settings	Identity Provider NetScaler	
Basic	Sign-in Page URL*	
Advanced	Verification Certificate Browse	
	Notification Email 4 Address	
	Custom login URL for your administrators: https://m4.maas360.com/login?custID=	
	Settings to configure in your SAML server Assertion Consumer Service URL: https://sso.connect.pingidentity.com/sso/sp/ACS.saml2 1 Entity Id: PingConnect 1	
Allow existing Administrators to use portal credentials as well.		
	O Authenticate against Corporate User Directory	
	Configure Strong Authentication	

7. Enter the values for the following fields:

Required Information	Description
Identity Provider Name*	NetScaler
Sign-in Page URL*	IdP logon URL
Verification Certificate	Upload the IdP certificate. Note : The IdP metadata is provided by Citrix and can be accessed from the link below. The link is displayed while configuring SSO settings for your app. <u>https://gateway.cloud.com/idp/saml/<citrixcloudcust id="">/<app id=""></app></citrixcloudcust></u> <u>/idp metadata.xml</u>
Notification Email Address	User's email address

8. Finally, scroll up and click **Save**.