Configuring Panorama9

Configuring Panorama9 for single sign-on (SSO) enables administrators to manage users of Citrix ADC. Users can securely log on Panorama9 by using the enterprise credentials.

Prerequisite

Browser Requirements: Internet Explorer 11 and above

To configure Panorama9 for SSO by using SAML:

- 1. In a browser, type <u>https://dashboard.panorama9.com</u> and press **Enter**.
- 2. On the home page, click **LOGIN**.
- 3. Type your Panoroma9 admin account credentials (Email and Password) and click Login.



Citrix Gateway

4. In the left panel, under **Client Dashboard**, click **Extensions**.

P											Ξ
	Client Dashboard						Client name filter All Columns O				
Client Dashboard	۵.	Client	+	•	Responsible	Vulnerabilities	Availability	Compliance	Server Issues	× •	Patch Issues
Templates		Totals	0	0		0	0	0	0	0	0
Extensions											
Client Groups											

5. In the **Extensions** page, click **Single Sign-On**.

6 %			
	Extensions		
Client Dashboard	API	0	Enable access via On Off
Templates	Zendesk	0	P9 API
The Extensions	Autotask	0	No API token
Create New Client	Desk.com	0	
Client Groups	Single Sign On	1	Create new API token
Script Repository	P9 Agent	0	
Export			
Messages			

6. Enter the values for the following fields:

Field	Description
Enable Single Sign-On	Select ON.
Certificate Fingerprint	Copy and paste the IdP certificate fingerprint from the <u>https://www.samltool.com/fingerprint.php</u> link, select Algorithm and Generate the Fingerprint .
Strict Validation	Select ON.
	Make note of Recipient attribute and Audience element, as it is required for IDP configuration.
Login URL	IdP logon URL
Consume URL	IdP issuer URL
Issuer	IdP issuer value

Extensions	;		
API	0	Enable Single	On Off
Zendesk	0	Sign-On	
Autotask	0	Identity URL	minut the Balance
Desk.com	0		The Panorama9 dashboard supports any SAML 2.0 compatible Identity Provider.
Single Sign-On	Т	Certificate	and the line of th
P9 Agent	0	fingerprint	
		Strict validation	On Off
			If enabled the recipient attribute and Audience element of the SAML Assertion must be issued to Panorama9. The SAML Assertion is generated by your Identity Provider as a part of the response to the Authentication request. This means your Identity Provider needs to know two things: 1) Recipient attribute: 2) Audience element: If disabled a bad Service Provider may reuse your SAML credentials to gain unauthorized access to
P9 Agent	0		your Panorama9 account.
		Login URL	I management where the second second
		Consume URL	CONTRACTOR OF CONTRACTOR
		Issuer	and the Restored
			If your Identity Provider uses a unified URL to handle all Single Sign-On requests, this issuer URI is sent as a part of the SAML authentication request. Copy it into e.g. the Entity ID field of your Identity Providers SAML setup.
			Save Changes

7. Finally, click **Save Changes**.