



EHOM Single Sign-On (SSO) Using Okta

Hosted Clients

Revised May 2022



©Net Health 2021.CONFIDENTIAL. All Rights Reserved.



Contents

What is SSO?	3
Requirements for Single Sign-On (SSO)	3
Net Health EHOM using Okta and Federation Authentication Services (FAS)	3
Okta integration with DUO	4
The Authentication Process	5
Overview	5
Okta configuration on the Customer Side	5





What is SSO?

Single sign-on (**SSO**) is an authentication scheme that allows a user to log in with a single ID to any of several related, yet independent, software systems.

True single sign-on allows the user to log in once and access services without reentering authentication factors.

Requirements for Single Sign-On (SSO)

Net Health EHOM using Okta and Federation Authentication Services (FAS)

Customers utilizing SSO will be provided a unique URL designated by Net Health. Customer will use this URL for the Okta application configuration on the General Settings page.

For General info on okta: <u>https://www.okta.com/</u>

Follow the "Configuring Okta" instructions outlined in the below URL to deploy "Citrix Gateway" application

- <u>https://support.okta.com/help/s/article/Citrix-NetScaler-Gateway-SAML-Configuration-Guide?language=en_US</u>
- Deploy "Citrix Gateway" Application in Okta
 - From Okta Console
 - Applications > Applications > Browse App Catalog

okta		Q barch	
4	~		
η	÷	III Applications	
nizationa	~	Create App Integration Browse App Catalog	Assign Users to App More *
ona	^		e for an application that can be assigned to your users.
leations		Q, Search	
nice		status 🕞	Okta Admin Console
	÷	ACTIVE 0	Octa Browser Plugin
	÷	INACTIVE 0	
	÷	•	Onta Deshboard
	~		





Select "Citrix Gateway"

okta		Q fauch.				O 38 month of	
Dechtorant	÷	= Back to Applications					
Directory	~	🗉 Browse App I	III, Browse App Integration Catalog				
Customizations	~	CATEGORIES		-			
Applications	~	Allintagrations	7942	C. City Galaxiey			
Applications		Analytics	675				
Bell Bernine		Appa Net Ganal	16	INTEGRATIONS			
		Collaboration and Photochurty	1245	Citrix Gateway			
hecusity	*	Developer Toxis	644	Othin Gateway (NADIU	°.		
Rickflow	*	Directories and HR Systems	204				
Reports v	~	Data Privacy and Consent Wanagement		GrifisMyPC (DRH)			
		Manager and		MyCitrix		SWA	
lattings	÷	Merily Greetance and		Citrix Receiver		5203	
		Administration	-	See All Results			
		Citatiand Marketing	738	T DILLA	4000011	C OHORSOS	
		tecurty	745	Stark.	Zuom	Microsoft Office 201	
		focial Login		Units, UAA, Processing	Unit, Protocorg	Int. ADVID. Processory	
		Jaco Trust Ecosystem					

- General Settings tab of "Citrix Gateway"
 - Use the Login URL provided by Net Health
- Select the Sign-On Tab
 - Ensure SAML 2.0 is in use
 - Click on 'View Setup Instructions' and provide the following information to Net Health
 - X.509 Certificate Link
 - Redirect URL
 - Single Logout URL
 - Issuer Name
 - o For Credentials Details
 - Application username format = Okta Username
- Import and Assign users for EHOH application
 - Use the EHOH username provided by Net Health
- NOTE FOR OKTA ADMIN: Only the EHOH users will have access to the system, you will not be able to successfully test login unless you have credentials within our system.

EHOM User list will be provided to Net Health along with the above info for SAML Config and certificate. Net Health will then complete EHOM user assignments within their systems and return user assignments to the Customer. The Customers Okta Admin will then complete the username assignments on their end.

Okta integration with DUO

Okta could perform LDAP authentication and DUO all before being handed back to Net Health systems and applications are presented. This would be controlled entirely by the customer. This is a configuration completely handled on the customer side.





The Authentication Process

Overview

A brief non-technical outline of how a user accesses Net Health infrastructure using their company credentials.

Citrix Netscaler communicates with Okta Citrix Gateway integration. FAS issues certs to users accessing the environment.

- User accesses custom Single Sign-On (SSO) URL
 - Netscaler identifies traffic and directs users to Okta portal
 - o Okta will authenticate user against Customer Active Directory
 - Okta returns with an assigned username to be used and a validated token for the user session
- SAML token passes authentication through Netscaler
 - Storefront issues a virtual smart card user certificate for user to access environment
 - Certificate is assigned to the username provided by Okta
- After authentication user is presented with applications
 - There's a setting within EHOM to enable single sign-on that must be enabled.
 - Okta username must match up with Active Directory username

Okta configuration on the Customer Side

Okta Documentation for Deployment:

https://help.okta.com/en/prod/Content/Topics/Directory/ad-agent-get-started.htm

- Register for Okta
- Okta will provide a URL used by the customer to manage the system
- Integrate Okta with Active Directory
 - Requires a service account to perform user actions

