

# FORUM SYSTEMS SENTRY<sup>TM</sup> VERSION 9.1 WEBADMIN OKTA INTEGRATION GUIDE



#### Legal Marks

No portion of this document may be reproduced or copied in any form, or by any means – graphic, electronic, or mechanical, including photocopying, taping, recording, or information retrieval system – without expressed permission from Forum Systems, Inc.

FORUMOS<sup>™</sup> Firmware, Forum Systems XMLSec<sup>™</sup> WebAdmin, Forum Systems XML Security Appliance<sup>™</sup>, Forum Sentry<sup>™</sup>, Forum Presidio<sup>™</sup>, Forum XWall<sup>™</sup>, Forum Sentry<sup>™</sup> Web Services Gateway, Forum Presidio<sup>™</sup> OpenPGP Gateway, Forum FIA Gateway<sup>™</sup>, Forum XWall Type-PCI<sup>™</sup>, Forum XWall<sup>®</sup> Web Services Firewall and Forum XRay<sup>™</sup> are trademarks and registered trademarks of Forum Systems, Inc.

All other products are trademarks or registered trademarks of their respective companies.

Copyright © 2002-2024 Forum Systems, Inc. - All Rights Reserved.

Forum Systems Sentry<sup>™</sup> Version 9.1 WebAdmin Okta Integration Guide, published January 2024.

D-ASF-SE-763233

# Table of Contents

OKTA CONFIGURATION	4
Overview	4
Prerequisite for Using Okta	4
Enable the Interaction Code Grant Type	4
Modify or Add an Authorization Server	5
Create a Web Application Policy	5
Create User Profile Attributes (Optional)	7
Privileged Access Attribute	8
Role Policy Attribute	9
Group Policy Attribute	9
Assign User Profile to Okta Users	10
Create OAuth Claims for the Custom Attributes	10
FORUM SENTRY OKTA WEB ADMIN INTEGRATION	12
Overview	12
Forum Sentry Okta User Policy	12
Okta User Policy Screen Terms	12
Okta User Policy Settings	13

# **OKTA CONFIGURATION**

#### Overview

This Guide will provide the minimum details required to support the Forum Sentry and Okta integration for Single Sign-On (SSO). If you don't have an Okta account, you can sign up for a developer account at https://developer.okta.com. Once you have access to an Okta account, you will need to configure the Authorization Server to support the Interaction Code grant then add a Web Application policy and configure the client credentials and interaction code.

#### Prerequisite for Using Okta

The Forum Sentry integration with Okta requires that you are using the Okta Identity Engine, not the Okta Classic Engine. If you are unsure which version of Okta you are using, you can verify whether you are on the Okta Identity Engine or the Classic Engine by following the below steps:

- 1. Log into the Okta Admin Dashboard.
- 2. Scroll down to the bottom of any Admin Dashboard page.
- 3. Look for the version number located at the bottom of the page.

The engine you are using is identified based on the version number. If the version number ends with an 'E', you are running on the Okta Identity Engine. If the version number ends with 'C', you are running on the Okta Classic Engine. For reference the version may look like this: Version 2023.12.1 E

If you have an Okta Classic Engine account you must upgrade it before proceeding.

#### **Enable the Interaction Code Grant Type**

Depending on the version of Okta you have, you may need to ensure you allow Administrators to configure the Interaction Code grant type on the Applications policy we will need later on. To check this setting, go to the Okta portal **Settings->Account** "Embedded widget sign-in support" widget and ensure the "Allow admins to configure the Interaction Code grant type for apps and authorization servers that they manage" option is checked.

🏥 okta		Q. Saurch for people, apps and groups:	⑦ □□ im <sup>·</sup> rumsys ∨
Dashboard Directory Customizations Applications Security Workflow		Client-based rate limiting Edit Prevent individual clients from blocking traffic on these scenarios. Learn more Cor view in System log 12 Client application Client a	Trust incidents and updates  Trust incidents and updates  Separate from Okta's provision of the Service, we will provide you with access to our support community and will communicate with you as an Okta Administrator (or Admin), including to send you Okta product and feature announcements, recommendations, and promotional offers. If you do not want to receive such communications, you may update your communications preferences by visiting our subscription center.
Reports Settings Account	~	OAuth 2.0 /authorize  C Enforce limit and log per client (recommended)  Log per client  Do nothing (not recommended)	Rate Limiting Communications Edit Enable Rate Limiting Communications Communications
Features Downloads		Embedded widget sign-In support Cancel Interaction Code Allow admins to configure the Interaction Code grant type for apps and authorization servers that they manage. Read more Ed Store	violation notification emails when this org meets rate limits.

#### Modify or Add an Authorization Server

Login to your Okta instance, go to **Security->API** menu and select the Authorization Server that you want to use for the Forum Sentry integration. You can choose to use the default instance, or create a new custom Authorization Server. To create a new Authorization Server, click on the "Add Authorization Server" button and use the following settings:

Name:	Sentry
Audience:	api://sentry
Description:	(optional)

Once the policy is created, ensure the Issuer setting is not set to dynamic, but rather a static URI.



#### **Create a Web Application Policy**

Login to your Okta instance, go to **Applications** menu and select the Create App Integration button. Under the Sign-In method, Choose "OIDC – OpenID Connect", and under the Application type setting, choose "Web Application".



On the following screen, name the policy (i.e. "MyForumSentry") and under **Grant Types** ensure that "Interaction Code" and "Refresh Token" are checked.

In the Sign-in redirect URIs section, add the following URI:

https://mysentry.mycompany.com:5050/webadmin/login/oktacallback

In the Trusted Origin section, add the following URI:

#### https://mysentry.mycompany.com:5050/

where *mysentry.mycompany.com* is the Hostname or IP address of the Sentry instance. Note that the redirect URI is case-sensitive.

Disclosed -   Directory •   Dustomizations •   Applications •   Sectory •   Applications •   Sectory •   Sectory<	🎇 okta		Q: Search for people, appx and groups		
Directory     Customizations     Applications     Applications     Applications     Set Service     AP Service integrations     AP Service integrations     AP Service integrations     Security	Dashboard	÷		App integration name	MyForumSentry
Customizations  Applications Applications Applications Set Service API Service Integration Security API Service Integration Security API Service Integration Security	Directory	~		Logo (Optional)	
Applications   Applications   Set Service   AP Service Integrations   Security   V   Workflow   V   Settings   Settings   Commentation Code   Settings   Settings <td>Customizations</td> <td>v</td> <td></td> <td></td> <td>Ø</td>	Customizations	v			Ø
Applications Grant type   Set: Service Client acting on behalf of itsef   API Service Integrations Client acting on behalf of a user:   acurity *   Nerkflow *   tettings *   Settings *   Sign-In redirect URIs Allow Widcard * in sign-In URI redirect.   Integration response and UD Integration codes   Sign-In redirect URIs Allow widcard * in sign-In URI redirect.   Integration codes Sign-In redirect URIs   Sign-In redirect URIs Integr/Imysentry.mycompany.com.5050/webadmin/login/oktacalib   Integr/Imysentry.mycompany.com.5050/webadmin/login/oktacalib Integr/Imysentry.mycompany.com.5050/webadmin/login/oktacalib   Allow Widcard * in sign-In URI redirect. Integr/Imysentry.mycompany.com.5050/webadmin/login/oktacalib   Integr/Imysentry.mycompany.com.5050/webadmin/login/oktacalib Integr/Imysentry.mycompany.com.5050/webadmin/login/oktacalib   Integr/Imysentry.mycompany.com.5050/webadmin/login/oktacalib Integr/Imysentry.mycompany.com.5050/webadmin/login/oktacalib   Integr/Imysentry.mycompany.com.5050/webadmin/login/oktacalib Integr/Imysentry.mycompany.com.5050/webadmin/login/oktacalib   Integr/Imysentry.mycompany.com.5050/webadmin/login/oktacalib Integr/Imysentry.mycompany.com.5050/webadmin/login/oktacalib   Integr/Imysentry.mycompany.com.5050/webadmin/login/oktacalib Integr/Imysentry.mycompany.com.5050/webadmin/login/oktacalib   Integr/Imysentry.mycompany.com.5050/webadmin/login/oktacalib Integr/Imysentry.mycompany.com.5050/webadmin/login/oktacalib   Integr/Imysentry.mycompany.com.	Applications	<u>.</u>			
Set Service   API Service Integrations   Security   Northflow   *   teports   *   Itettings   *   Sign-in redirect URis   Allow wildcard * in sign-in URI redirect:   https://mysentry.mycompany.com/S050/webadmin/login/lokitacalib   Citer in Filter Boken   Sign-out redirect URis   Allow wildcard * in sign-in URI redirect:   https://mysentry.mycompany.com/S050/webadmin/login/lokitacalib   Verter Cd   Https://mysentry.mycompany.com/S050/webadmin/login/lokitacalib	Applications			Grant type	Client acting on behalf of itself
API Service Integrations leacurity  API Service Integrations leacurity  Kentriker C  Authoritzation Code  Authoritzation Code  Authoritzation Code  Authoritzation Code  Authoritzation Code  Service Integration  Sign-in redirect URIs  Allow wildcard * in sign-in URI redirect.  Allow wildcard * in sign-in URI redirect.  Integr/mysentry.mycompany.com.5050/webadmin/togic/okitacallb  Learn More C  Sign-out redirect URIs  Sign-out redirect URIs  Allow Wildcard * in sign-in URI redirect.  Learn More C  Trusted Origins  Beau IDIR (Cotinent)  Allow Vildcard * in sign-in URI redirect.  Exam More C  Trusted Origins  Beau IDIR (Cotinent)  Allow Vildcard * in sign-in URI redirect.  Allow Vildcard * in sign-in URI red	Self Service			Learn More F2	Client Credentials
API Service Integrations <ul> <li>Activation Code</li> <li>Matrixation Code</li> <li>Matrixat</li></ul>					Client acting on behalf of a user
scurity       v         birthow       v         sports       v         stings       v         Sign-in redirect UBis       Allow wildcard * in sign-in UBI redirect:         Oxia sends the authentication response and ID       https://mysentry.mycompany.com/5050/webadmin/login/oktracatib         Learn More E3       + And UBi         Sign-out redirect UBis (Optional)       http://dcalhost:8080         Atter your application contacts Oxia the user to one of the UBis       http://dcalhost:8080         Learn More C3       Trusted Origins         Resulting (Control)       http://calhost:8080	API Service Integrati	ons			Authorization Code
In Referent Token   inports   vettings   <	ecurity	~			Value Interaction Code
exitings					Sefresh Token
ports v  ttings v  Sign-in redirect URis Gita sanda the aichaedication response and O tokens for the user's sign-in regirect to these URis Learn More C  Sign-out redirect URis (Optional) After your application contacts Obta to close the user session, Obta redirects the user to one of these URis Learn More C  Trusted Origins  Rate URIs (Optional)	orkflow	~			Client-initiated backchannel authentication flow (CIBA)
titings       Sign-in redirect URis       Allow wildcard * in sign-in URi redirect.         Dita sends the authentication response and ID taken for the user's sign-in request to these URis       https://mysentry.mycompany.com.5050/webadmin/login/oktacallb         Learn More Cl       + Add URi         Sign-out redirect URis (Optional)       http://localnost.8080         Atter year application contacts Data to close the user's sign-in water to one of these URis       http://localnost.8080         Trusted Origins       Rate URit (Ontional)         Rate URIt (Ontional)       Rate URIt (Ontional)	ports				Of antipate of cardy.
Okta senda the authentication response and ID token for the user's sign-to request to these URIs       https://mysentry.mycompany.com/S050/webadmin/login/oktacatib         Learn More I2       + Aod URI         Sign-out redirect URIs (Optional)       http://localhost.8080         Atter your application contacts Data to close the user sestion, Okta redirects the user to one of these URIs       http://noralhost.8080         Learn More I2       -         Trusted Origins       -         Base URIs       (Inclose)	ttings			Sign-in redirect URIs	Allow wildcard * in sign-in URI redirect.
Learn More C3 + Add UR Sign-out redirect URIs (Optional) After your application contacts Okta to close the user session. Okta redirects the user to one of these URIs. Learn More C3 Trusted Origins Base URIs (Optional)				Okta sends the authentication response and ID token for the user's sign-to request to these URIs	https://mysentry.mycompany.com:5050/webadmin/login/oktacalib
Sign-out redirect URIs (Optional) After your application contacts (Atta to close the user present). Obta redirects the user to one of these URIs. Learn More C Trusted Origins Rese URI				Learn More 12	+ Add URI
After your application contacts Data to close the user session, Data redirects the user to one of These URE. Learn More [2]				Sign-out redirect URIs (Optional)	http://localhost:8080
Learn More (3 Trusted Origins				After your application contacts Okta to close the user session, Okta redirects the user to one of these URIs.	+ Add URI
Trusted Origins				Learn More C	
Base ( Dire ( Orthogal)				Trusted Origins	
https://mysentry.mycompany.com:5050				Base URIs (Optional)	https://mysentry.mycompany.com:5050

## **Create User Profile Attributes (Optional)**

Sentry supports 3 custom attributes for users logging into the WebAdmin from Okta. These attribute names are configurable on the Sentry Okta policy, so you can choose to user your own custom attribute names for these, but they need to be set both in the Sentry Okta Policy and be set properly under the Okta **Directory->Profile Editor** section for the Forum Sentry application profile. If you choose to use these optional features, the custom attributes can using the steps below.

THE ONLO	Q. Search for people,	abbs and Buonba		0	88 ~
Dashboard × Directory ^	Profile Editor				• Help
People Groups Devices Profile Editor Directory Integrations Profile Sources	Learn about Univ Universal Direct: Using Profiles All of th Go to Document Users Groups	ersal Directory ory allows you to sto tor, you can extend a ese features provide ation	re employee, partner, and customer profiles in and customize user and app-specific profiles, robust provisioning support.	n Okta, generating a user-bi as well as transform and m	o ised, single source of truth. ap attributes between
Customizations ~	Users				
Applications V	Q. Search				<ul> <li>Create Okta User Type</li> </ul>
Security 🗸	Filters	Profile		Туре	
Workflow ~	Okta	okta	User (default) user	Okta	
Reports ~	Apps	d-anno	Developer Registration SSO User oldc_idp	Identity Provider	Mappings
Settings 🗸	Identity Providers	0	MyForumSentry User oldc_client	Application	Mappings

1) Go to the Directory->Profile Editor section and clicking on the Sentry Application profile.

#### **Privileged Access Attribute**

The Privileged Access Attribute is an attribute defined for the Okta user which will be used to determine whether the Web Admin user will be granted privileged access (i.e. super user) rights. By default, any user authenticated through Okta has privileged access. If there is an attribute specified in Okta and Sentry for the privileged access attribute, the user will only have privileged access if the Boolean attribute exists with value = true.

1) To create the Privileged Access custom attribute, go to the Sentry application profile screen shown above and click the "Add Attribute" button to bring up the new attribute dialog

🗱 okta		Q. Search for people.	apps and groups			0 ==		
irectory People	~	← Back to profiles Profile Editor						
Groups Devices		MyForumSentry	User		🖍 Edit	Ø		
Profile Editor		Display name	MyForur	mSentry User		MyForumBa	MY.	
Directory Integratio	ns	Description						
Profile Sources		Variable name	oidc_c1	ient				
stomizations	~							
plications	<b>*</b>	Attributes						
curity	~	+ Add Attribute	Mappings					
rkflow	Ť	Filters	Display Name	Variable Name	Data type	Attribute Type		
orts	v	All	Username	userName	string	Base	0	×
lings	~	Base Custom	Name	name	string	Base	0	×
			Nickname	nickname	string	Base	0	×
			Given Name	civen name	strina	Base	0	×

2) Choose Data Type "boolean" and provide a display name and a variable name for the attribute, such as: **sentry\_privileged\_access** 

You can then choose the User permissions for this attribute. It is recommended to use Read Only to prevent users from setting their own attribute values.

Add	Attribute
71010	Autorio

*Local app attributes are only store attributes if you plan to add the attri value in Okta.	ed on Okta and not created in MyForumSentry. Use local bute to MyForumSentry or only want to store the mapped
Data type	boolean +
Display name	sentry_privileged_access
Variable name	sentry_privileged_access
Description	
Attribute required	O Yes
Scope	User personal
User permission	<ul> <li>Hide</li> <li>Users cannot view the attribute. Select this option to hide sensitive attributes. For example, salary information</li> <li>Read Only</li> <li>Users can view the attribute, but attribute properties cannot be modified. Select this option to prevent attribute properties from changing. For example, a title</li> </ul>

#### **Role Policy Attribute**

The Role Policy Attribute is an attribute defined for the Okta user which will be used to determine the Role Policy from Forum Sentry that the Web Admin user will be granted on login. By default, no role policy is assigned to an Okta user if a Role Attribute does not exist. If there is a Role Policy value configured for the role attribute and the value is not empty, a role policy is required to exist in Sentry or the authentication will be denied. It is allowed for the attribute to not exist (default) or to have an empty value.

1) To create this custom attribute, from the Sentry application profile screen shown above, click the "Add Attribute" button to bring up the new attribute dialog

2) Choose Data Type "string" and provide a display name and a variable name for the attribute, such as: **sentry\_role\_policy** 

Local app attributes are on attributes if you plan to add t value in Okta.	ly stored on Okta and not cre he attribute to MyForumSent	ated in MyForumSentry. Use k ry or only want to store the ma	ical ipped
Data type	string	•	
Display name 🛛	sentry_role_polic	У	
Variable name	sentry role polic	v	

You can then choose the User permissions for this attribute. It is recommended to use Read Only to prevent users from setting their own attribute values.

#### **Group Policy Attribute**

The Group Policy Attribute is an attribute defined for the Okta user which will be used to determine the Group Policy from Forum Sentry that the Web Admin user will be associated with on login. By default, no group policy is configured. If there is an attribute configured for the group policy and the value is not empty, a group policy is required to exist in Sentry. It is allowed for the attribute to not exist (default) or to have an empty value.

1) To create this custom attribute, from the Sentry application profile screen shown above, click the "Add Attribute" button to bring up the new attribute dialog

2) Choose Data Type "string" and provide a display name and a variable name for the attribute, such as: **sentry\_group\_policy** 

Add Attribute		
*Local app attributes are on attributes if you plan to add t value in Okta.	ly stored on Okta and not crea he attribute to MyForumSentr	ated in MyForumSentry. Use local ry or only want to store the mapped
Data type	string	•
Display name 🛛	sentry,group_po	licy
Variable name	sentry_group_pol	licy

You can then choose the User permissions for this attribute. It is recommended to use Read Only to prevent users from setting their own attribute values.

## Assign User Profile to Okta Users

If you choose to use these custom attributes, then once then steps above have been completed to create these attribute types for the Okta user profiles, you will then need to assign the values for these attributes on the user policies defined in Okta. To do this, go to **Directory->People**, click on the People policy and then click the "Assign Applications" button.

يَّة oktα		$\boldsymbol{Q}_{\!\!\boldsymbol{A}}$ Search for people, apps and groups
Dashboard	~	test user
Directory	^	testuser@company.com
People		C Resend Password Email More Actions *
Groups		🛓 User 🛛 🔺 Password expired. User is now in one-time password ı
Profile Editor		Applications Groups Profile Devices
Directory Integrations		Assigned Applications
Profile Sources		Assign Applications
Customizations	~	Application Assignment & App Us
Applications	~	

On the subsequent dialog, click the Assign link next to the Sentry application.

Assign Applications				
Q Search				
MyForumSentry	Assign			

The resulting "Assign Applications" dialog will show all of the User attribute values that can be set, including the 3 new custom attributes created in the steps above. These values should correspond to the Forum Sentry Okta Policy and Sentry WebAdmin expected values. Please refer to the section below for more information on these optional values and their usage.

Note that the "Assign Applications" step will not be allowed if you have Federation Broker Mode enabled on your application. Please refer to Okta documentation if you choose to have Federation Broker Mode enabled and want to assign attribute values to individual users.

#### **Create OAuth Claims for the Custom Attributes**

In order for Okta to send the attributes and values to Sentry for the users, each custom attribute will require a new claim to be added under **Security->API->Authorization Servers**. Click on the Authorization Server you are using for Sentry, then click the Claims tab and the "Add Claim" button.



Each attribute will require a new claim to be added under Security->API->Authorization Servers.

#### 1) Create the Claim for the Privileged Access attribute

Name: sentry\_privileged\_access Include in token type: ID Token / Always Value Type: Expression Value: (appuser != null) ? appuser.sentry\_privileged\_access : false Include In: Any Scope

#### 2) Create the Claim for the Role Policy attribute

Name: sentry\_role\_policy Include in token type: ID Token / Always Value Type: Expression Value: (appuser != null) ? appuser.sentry\_role\_policy : "" Include In: Any Scope

#### 3) Create the Claim for the Group Policy attribute

Name: sentry\_group\_policy Include in token type: ID Token / Always Value Type: Expression Value: (appuser != null) ? appuser.sentry\_group\_policy : "" Include In: Any Scope

Note: Any name can be used for the attributes. The attribute names listed here are suggestions. Any value can be configured in Okta and then referenced in the Sentry Okta Policy (see steps below).

# FORUM SENTRY OKTA WEB ADMIN INTEGRATION

#### Overview

Forum Sentry provides an Okta adapter policy to enable login to the Web Admin interface via Okta. Please be sure to complete the steps in the <u>Okta Configuration</u> section above before continuing with this section.

## Forum Sentry Okta User Policy

Login to the Forum Sentry Web Admin and go to the **Access->User Policy** menu. Here there will be a link "Okta" for provisioning the Sentry Web Admin users to be able to login via Okta.

FORUMSERLAY	> API SECURITY GATEWAY	C FORUMSYSLEMS
GENERAL Forum Systems	0 K TA	
Getting Started Help	OKTA POLICY	
DIAGNOSTICS	Name:	WebAdminOktaPolicy
	Issuer:*	https://dev-77β27793.okta.com/oauth2/ausecpj225UJGHV9g5d7
GATEWAY	Client ID:*	0oaed4oybpl8vURpH5d7
RESOURCES	Client Secret:	
IDP	Privileged Access Attribute:*	sentry_privileged_access
ACCESS	Role Policy Attribute:*	sentry_role_policy
Runtime Access User ACLs	Group Policy Attribute:*	sentry_group_policy
HOSTACLS IP ACLS XACML	Enable Diagnostics Logging:	
Admin Access Domains Roles User Policies Users Cache User Groups Active Users LDAP RSA Securiti Kerberos SiteMinder WebSeal Oracle AM WS-Trust OpenAM REST Sentry Custon Okta		Reset Test Save

#### **Okta User Policy Screen Terms**

Here are the screen options you will find under the Okta menu.

FIELD NAME	DEFINITION
Name	WebAdminOktaPolicy (not configurable)
Issuer	The issuer URI defined in Okta
Client ID	The Client ID is the public identifier for the Okta Application policy.

Client Secret	The Client Secret is a secret known only to the application and the Okta authorization server.
Privileged Access Attribute	An attribute defined for the Okta user which will be used to determine whether the Web Admin user will be granted privileged access (i.e. super user) rights. By default, any user authenticated through Okta has privileged access. If there is an attribute configured for privileged access attribute in the Okta policy, the user will only have privileged access if the Boolean attribute exists for the user with value = true.
Role Policy Attribute	An attribute defined for the Okta user which will be used to determine the Role Policy from Forum Sentry that the Web Admin user will be granted on login. By default, no role policy is configured. If there is an attribute configured for the role policy and the value is not empty, a role policy is required to exist in Sentry. It is allowed for the attribute to not exist or to have an empty value.
Group Policy Attribute	An attribute defined for the Okta user which will be used to determine the Group Policy from Forum Sentry that the Web Admin user will be associated with on login. By default, no group policy is configured. If there is an attribute configured for the group policy and the value is not empty, a group policy is required to exist in Sentry. It is allowed for the attribute to not exist or to have an empty value.
Enable Diagnostic Logging	Enables debug logging for Okta authentication sequences.

# **Okta User Policy Settings**

After configuring the Okta policies from the sections above, these values will need to be entered for the Forum Sentry Okta policy.

	· · · · · · -
FIELD NAME	VALUE
lssuer	The issuer URI from the Okta found under the Security -> API -> Authorization Servers for the authorization policy that will be handling these requests.
Client ID	Client ID value as shown in the Okta Applications->[SentryWebApplication] policy.
Client Secret	Client Secret value as shown in the Okta Applications->[SentryWebApplication] policy.
Privileged Access Attribute	<ul><li>(Optional). The Okta custom variable name that is to be used to determine Privileged Access for the user. If no value is specified, any user authenticated via Okta will be granted Privileged Access rights.</li><li>Note: The presence of a Role Policy attribute or Group Policy attribute properly configured will automatically disable privileged access even if granted via this attribute.</li></ul>
Role Policy Attribute	(Optional). The Okta custom variable name that is to be used to determine which Role Policy to associate to the Okta user. If no value is specified or no attribute is defined, no Role Policy will be associated.
Group Policy Attribute	(Optional). The Okta custom variable name that is to be used to determine which Group Policy to associate to the Okta user. If no value is specified or no attribute is defined, the no Group Policy will be associated.
Enable Diagnostic Logging	Checked for debug diagnostic logging, unchecked for standard logging.

# Sample values for Okta Policy:

Issuer:	https://dev-62563068.okta.com/oauth2/default
Client ID:	0oactaa5ghcWtEdcc5d7
Client Secret:	B0wWYrJxPNL-avjeUhPJ2S6j4AL0sqb5FULNUjKD10IOfW\
<b>Privileged Access Attribute:</b>	sentry_privileged_access
Role Policy Attribute:	sentry_role_policy
Group Policy Attribute:	sentry_group_policy