



FORUM SENTRY™ VERSION 9

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.

FORUMOST™ Firmware, Forum Systems XMLSec™ WebAdmin, Forum Systems XML Security Appliance™, Forum Sentry™, Forum Presidio™, Forum XWall™, Forum Sentry™ Web Services Gateway, Forum Presidio™ OpenPGP Gateway, Forum FIA Gateway™, Forum XWall Type-PCI™, Forum XWall® Web Services Firewall and Forum XRay™ 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 Sentry™ Version 9 WebAdmin Okta Integration Guide, published Oct 2024.

D-ASF-SE-763235

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	7
Create User Profile Attributes (Optional)	8
Privileged Access Attribute.....	9
Role Policy Attribute	10
Group Policy Attribute	10
Assign User Profile to Okta Users.....	11
Create OAuth Claims for the Custom Attributes	11
FORUM SENTRY OKTA WEB ADMIN INTEGRATION.....	13
Overview	13
Forum Sentry Okta User Policy	13
Okta User Policy Screen Terms	13
Okta User Policy Settings	14

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:

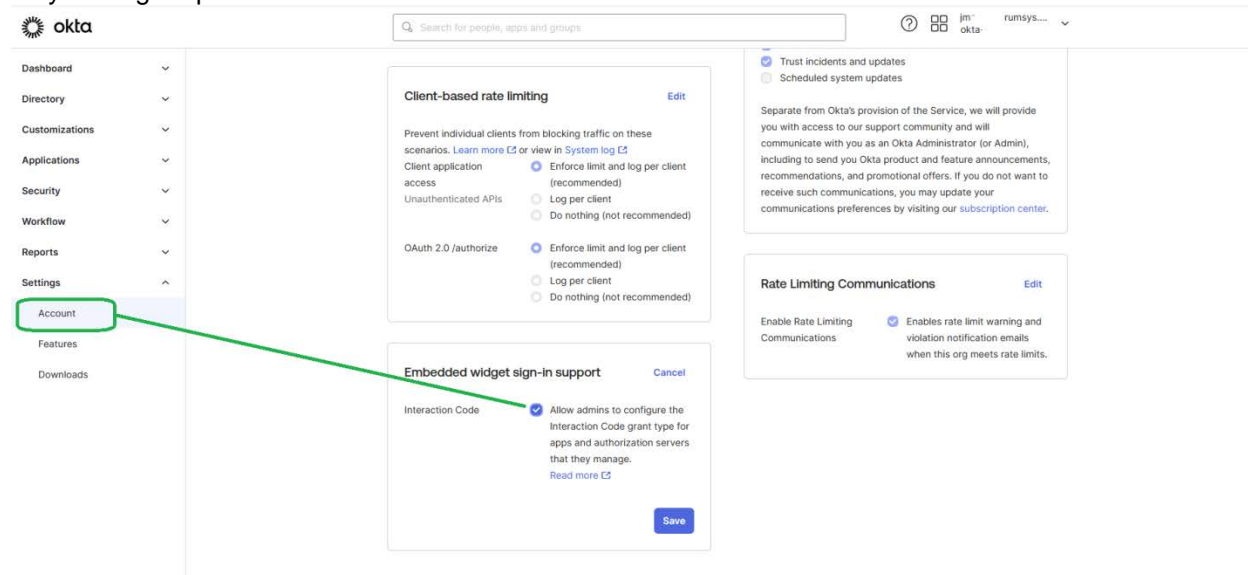
1. Log into the Okta Admin Dashboard.
2. Scroll down to the bottom of any Admin Dashboard page.
3. Look for the version number located at the bottom of the page.

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.

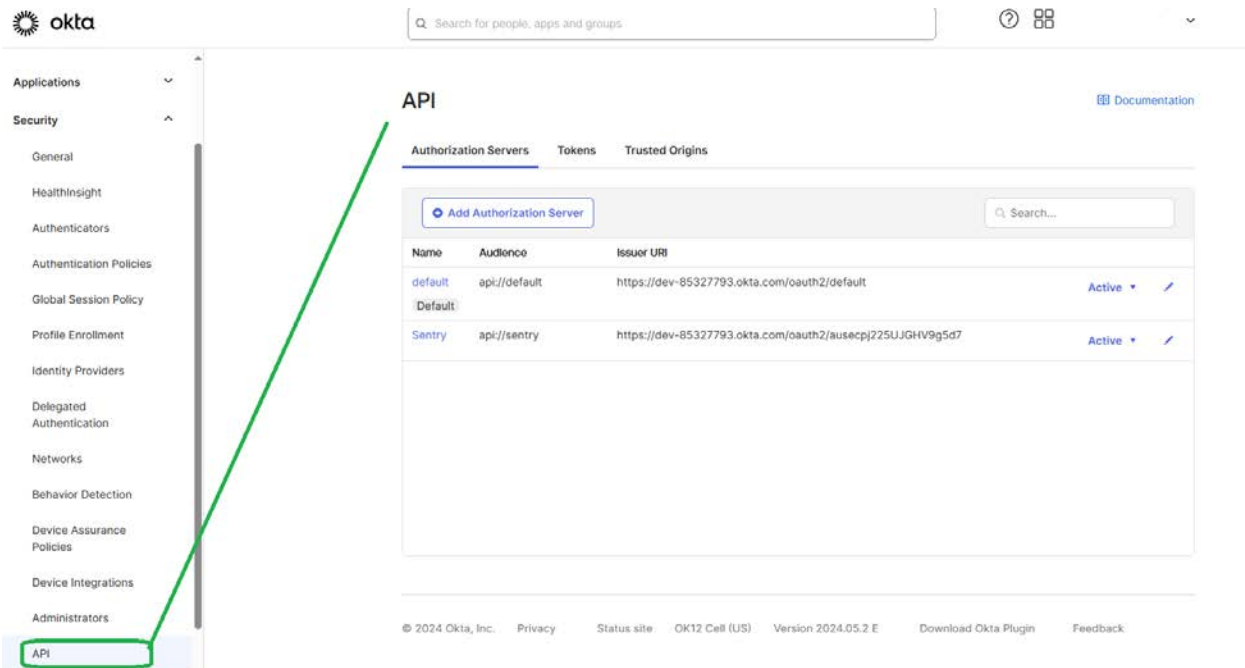


Modify or Add an Authorization Server

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.



Add a new Access Policy for the Authorization Server

Go to **Security->API** menu and click on the Authorization Server that you want to use for the Forum Sentry integration. Go to the **Access Policies** Tab and create a new Access Policy called “AuthorizeSentry”.

Settings Scopes Claims **Access Policies** Token Preview

Add New Access Policy

1
AuthorizeSentry

AuthorizeSentry

Active

Edit

Delete

Description

Authorize Forum Sentry Instances

Assigned to clients

All Clients

Add rule

Priority	Rule Name	Scopes	Status	Actions
1	test	All	Active	<div></div> <div></div> <div></div>

Click on the Add Rule button and use the following settings:

Rule Name

sentry

IF

Grant type is

Client acting on behalf of itself

☒ Client Credentials

Client acting on behalf of a user

☒ Authorization Code
☒ Interaction Code
☒ Implicit (hybrid)
☒ Resource Owner Password
☐ SAML 2.0 Assertion
☐ Device Authorization
☐ Token Exchange
☐ Client-initiated backchannel authentication flow (CIBA)

AND

User is

☒ Any user assigned the app
☐ Assigned the app and a member of one of the following:

AND

Scopes requested

☒ Any scopes
☐ The following scopes:

THEN

Use this inline hook

None (disabled)

AND

Access token lifetime is

1

Hours

AND

Refresh token lifetime is

Unlimited

but will expire if

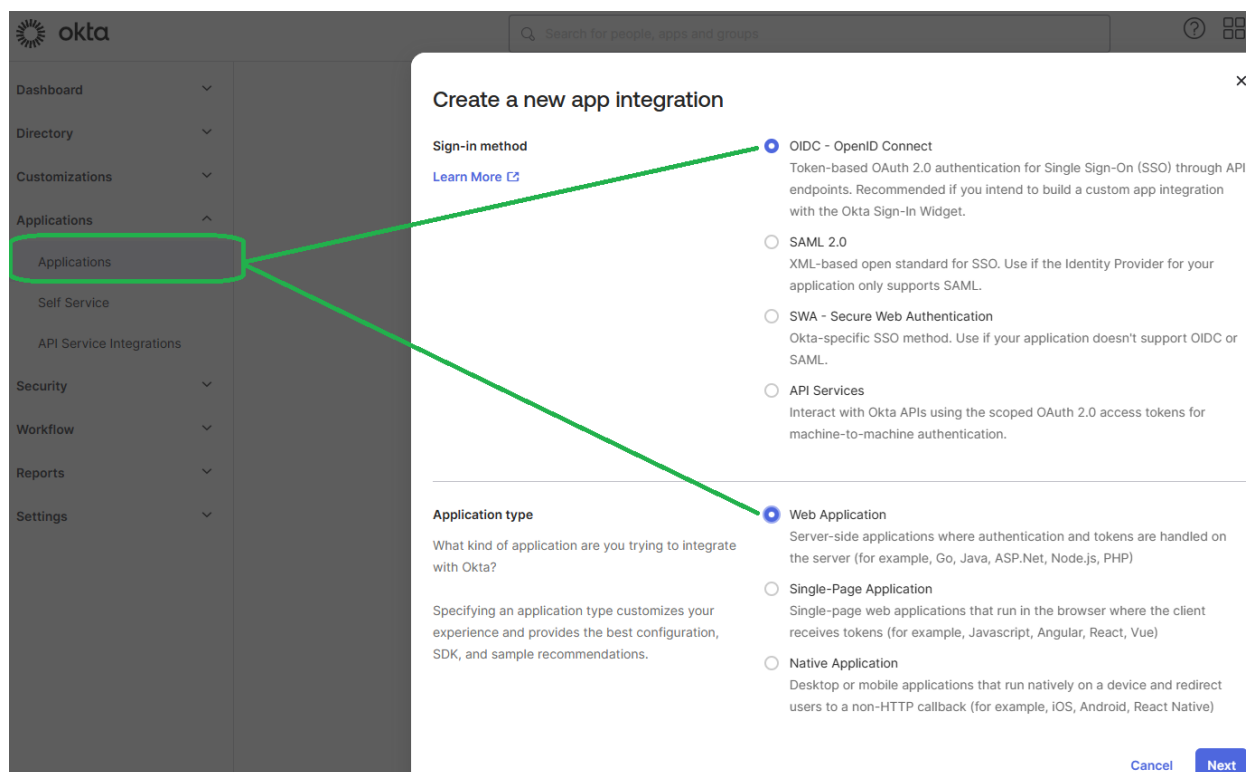
7

Days

6 | Forum Sentry™ WebAdmin Okta Integration Guide

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.

App integration name MyForumSentry

Logo (Optional)

Grant type

Client acting on behalf of itself

- ☐ Client Credentials

Client acting on behalf of a user

- ☒ Authorization Code
- ☒ Interaction Code
- ☒ Refresh Token
- ☐ Client-initiated backchannel authentication flow (CIBA)
- ☐ Implicit (hybrid)

Sign-in redirect URIs

Okta sends the authentication response and ID token for the user's sign-in request to these URIs

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

Sign-out redirect URIs (Optional)

After your application contacts Okta to close the user session, Okta redirects the user to one of these URIs.

http://localhost:8080

Trusted Origins

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 use 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.

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

Profile Editor

Learn about Universal Directory

Universal Directory allows you to store employee, partner, and customer profiles in Okta, generating a user-based, single source of truth. Using Profile Editor, you can extend and customize user and app-specific profiles, as well as transform and map attributes between profiles. All of these features provide robust provisioning support.

Go to Documentation

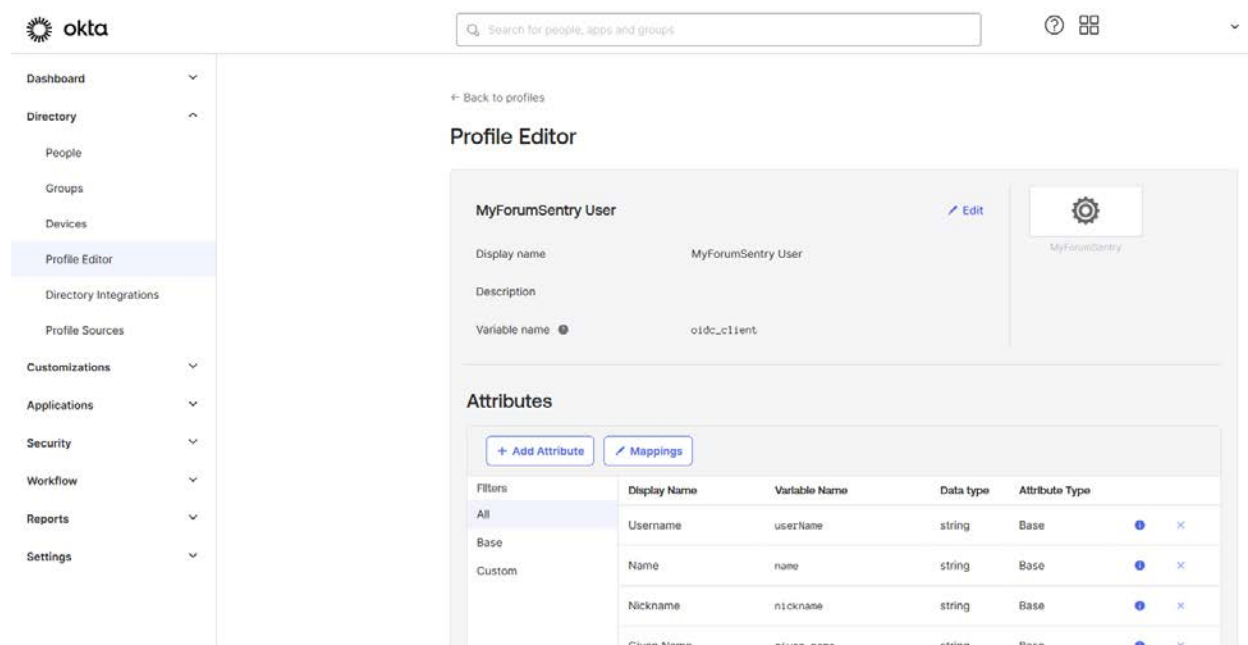
Users

Profile	Type
okta User (default) user	Okta
Developer Registration SSO User oldc_idp	Identity Provider
MyForumSentry User oldc_client	Application

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



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

* Local app attributes are only stored on Okta and not created in MyForumSentry. Use local attributes if you plan to add the attribute to MyForumSentry or only want to store the mapped value in Okta.

Data type: boolean

Display name: sentry_privileged_access

Variable name: sentry_privileged_access

Description:

Attribute required: ☐ Yes

Scope: ☐ User personal

User permission: ☒ Read Only

Users cannot view the attribute. Select this option to hide sensitive attributes. For example, salary information

Users can view the attribute, but attribute properties cannot be modified. Select this option to prevent attribute properties from changing. For example, a title

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**

Add Attribute

* Local app attributes are only stored on Okta and not created in MyForumSentry. Use local attributes if you plan to add the attribute to MyForumSentry or only want to store the mapped value in Okta.

Data type: string

Display name: sentry_role_policy

Variable name: sentry_role_policy

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 only stored on Okta and not created in MyForumSentry. Use local attributes if you plan to add the attribute to MyForumSentry or only want to store the mapped value in Okta.

Data type: string

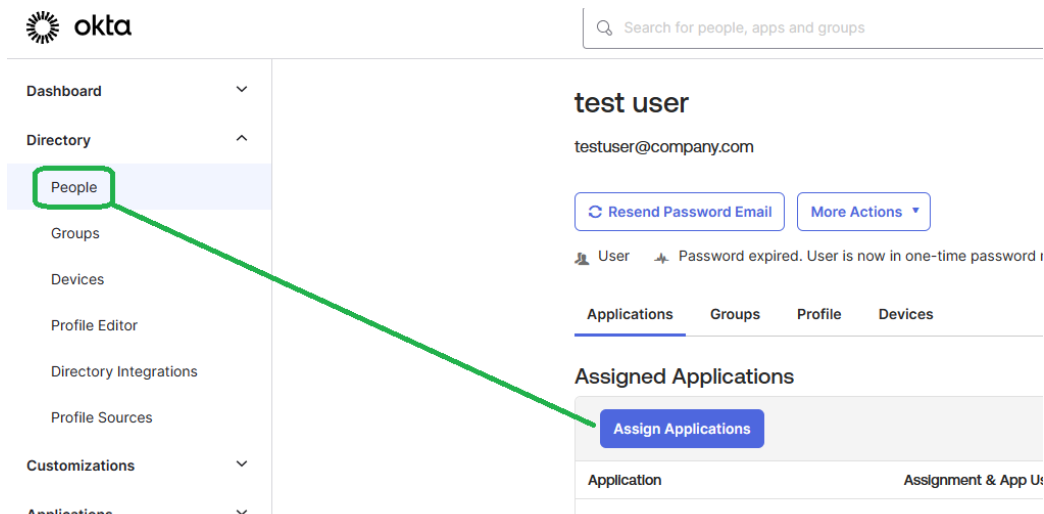
Display name: sentry_group_policy

Variable name: sentry_group_policy

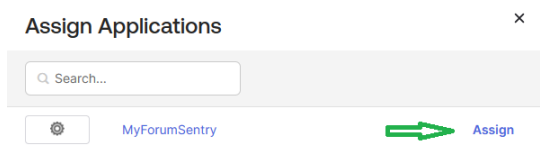
You can then choose the User permissions for this attribute. It is recommended to use Read Only to prevent users from setting their own attribute values.

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.



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

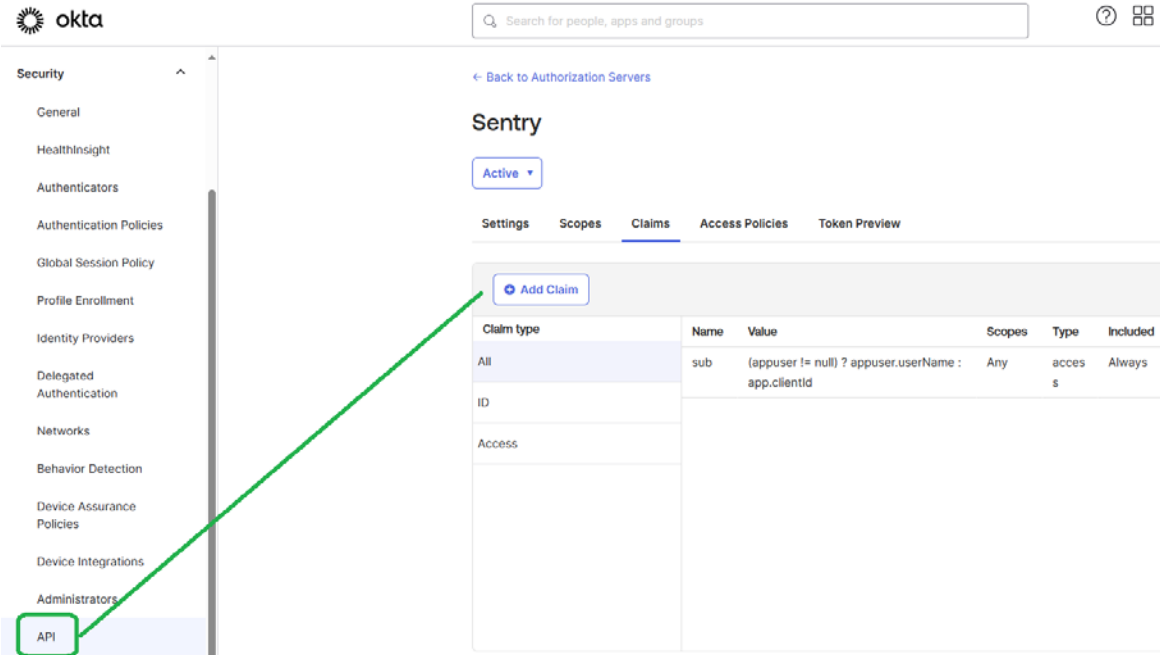


The resulting “Assign Applications” dialog will show all of the User attribute values that can be set, including the 3 new custom attributes created in the steps above. These values should correspond to the Forum Sentry Okta Policy and Sentry WebAdmin expected values. Please refer to the section below 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 [Okta Configuration](#) 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.

The screenshot displays the Forum Sentry Web Admin interface. The left sidebar menu includes sections like GENERAL, DIAGNOSTICS, GATEWAY, RESOURCES, IDP, and ACCESS. Under the ACCESS section, there are sub-menus for Runtime Access, Admin Access, and User Policies. The 'Okta' link under User Policies is highlighted with a green box. A green arrow points from this link to the 'OKTA POLICY' section header in the main content area. The 'OKTA POLICY' form contains the following fields:

- Name: WebAdminOktaPolicy
- Issuer: <https://dev-77327793.okta.com/oauth2/ausecpj225UJGHV9g5d7>
- Client ID: 00aed4oybpl8vURpH5d7
- Client Secret: (empty field)
- Privileged Access Attribute: sentry_privileged_access
- Role Policy Attribute: sentry_role_policy
- Group Policy Attribute: sentry_group_policy
- Enable Diagnostics Logging: ☒

At the bottom right of the form are buttons for 'Reset', 'Test', and '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
Issuer	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	(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. 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.
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\
Privileged Access Attribute: sentry_privileged_access
Role Policy Attribute: sentry_role_policy
Group Policy Attribute: sentry_group_policy