

UNCLASSIFIED



# **OKTA IDENTITY AS A SERVICE (IDAAS) DOD WARNING BANNER CONFIGURATION**

**Version 1, Release 1**

**22 April 2025**

**Developed by Okta and DISA for the DOD**

UNCLASSIFIED

### **Trademark Information**

Names, products, and services referenced within this document may be the trade names, trademarks, or service marks of their respective owners. References to commercial vendors and their products or services are provided strictly as a convenience to our users, and do not constitute or imply endorsement by the Defense Information Systems Agency (DISA) of any nonfederal entity, event, product, service, or enterprise.

## TABLE OF CONTENTS

	<b>Page</b>
<b>1. INTRODUCTION.....</b>	<b>1</b>
<b>2. DOCUMENTATION .....</b>	<b>2</b>
<b>3. INSTRUCTION.....</b>	<b>3</b>
3.1 Creating a Brand .....	3
3.2 Adding a Custom Domain .....	4
3.3 Modifying the Sign-In Page.....	5

## 1. INTRODUCTION

To configure the DOD Warning Banner within Okta, implementers must modify the sign-in page by adding a small Javascript snippet that presents the banner and gives the option to click “OK”. Implementing the notice and banner requires setting a Custom Domain, which unlocks the ability to modify the sign-in page.

The step-by-step instructions below address creating a brand (custom site graphics and design), configuring a custom domain name, and editing the sign-in page. Additional information can be found in the Okta online documentation by following the links below.

## 2. DOCUMENTATION

Set a brand for the organization:

- <https://help.okta.com/oie/en-us/content/topics/settings/branding-set-theme.htm>

Configure a custom domain and email address:

- <https://help.okta.com/oie/en-us/content/topics/settings/settings-configure-custom-url.htm>
- <https://developer.okta.com/docs/guides/custom-url-domain/main/>

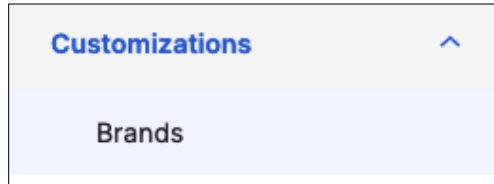
Customize the sign-in page:

- <https://help.okta.com/oie/en-us/content/topics/settings/branding-pages.htm>

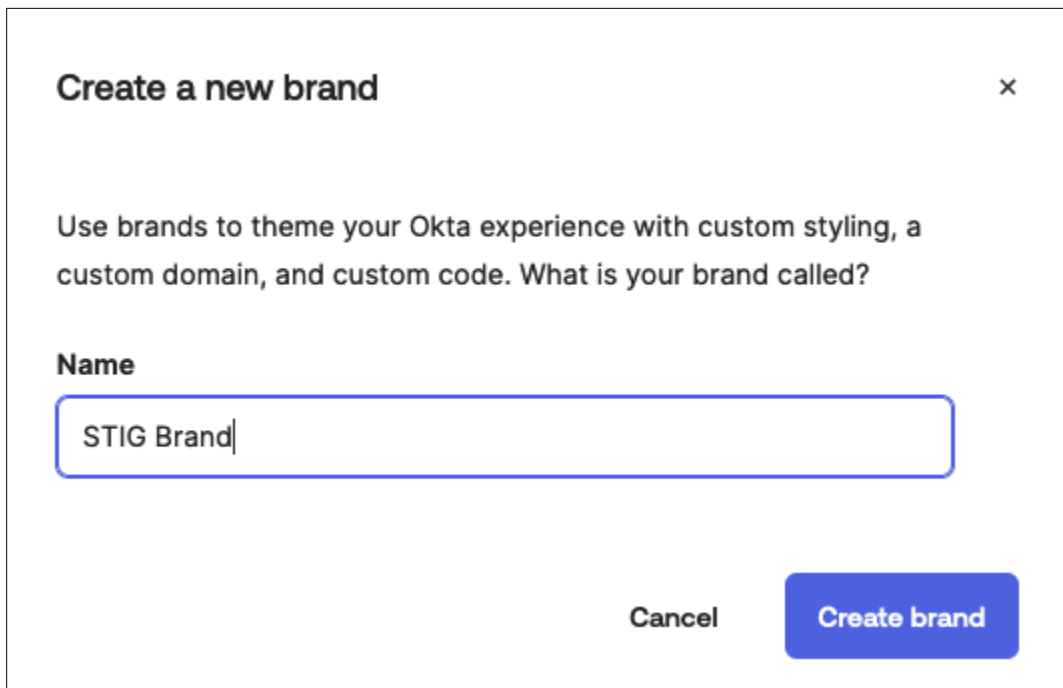
### 3. INSTRUCTION

#### 3.1 Creating a Brand

1. Log in to the admin console.
2. Click Customizations >> Brands.



3. Click **+ Create Brand**.
4. Give the Brand a name and click **Create Brand**.

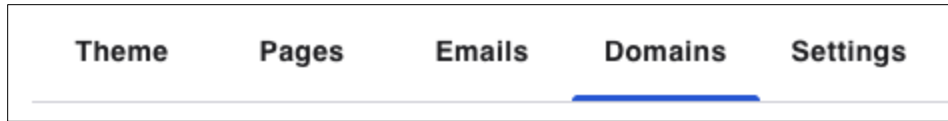
A screenshot of a modal dialog box titled 'Create a new brand' with a close button (X) in the top right corner. The dialog contains the text: 'Use brands to theme your Okta experience with custom styling, a custom domain, and custom code. What is your brand called?'. Below this text is a label 'Name' followed by a text input field containing the text 'STIG Brand'. At the bottom right of the dialog are two buttons: 'Cancel' and 'Create brand'.

5. Click on the newly created Brand.

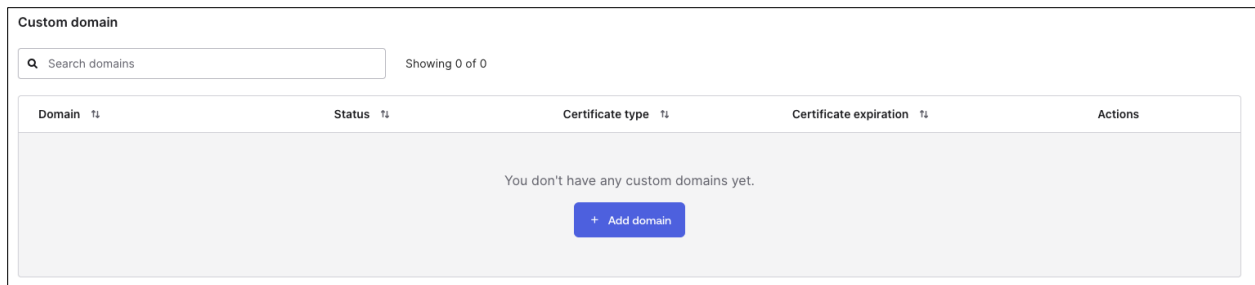


### 3.2 Adding a Custom Domain

1. In the **Brand**, click **Domains**.



2. Under **Custom Domains**, click **Add Domain**.



3. In the **Add domain** screen, enter the fully qualified domain name the organization would like to use. This would be a subdomain of a domain the organization owns.

### Add domain

The custom domain you add can be used in addition to your organization's standard Okta domain.

The issuer mode of Identity Providers, Authorization Servers, and OIDC Apps will be automatically changed to your custom domain.

To get this domain working, you'll need to edit DNS records at your registrar or DNS provider.

[Docs](#)

**Domain**

stig. [redacted] com

Your fully-qualified domain name. For example: login.example.com

**Certificate management**

☒ **Okta-managed (faster and easier)**

Okta will provision and renew TLS certificates for your domain automatically, which is less work for you.

☐ **Bring your own certificate (advanced)**

You have your own PEM-encoded certificate, private key, and certificate chain. Before it expires, you'll need to return and provide an updated certificate manually.

#### Notes:

- To comply with FIPS regulations, you **MUST** choose **Bring your own certificate (advanced)**.

- You will need access to and the privileges to modify the DNS records for your domain and will have to set up a certificate on that domain for use in this process.
- Setting up a certificate and modifying specific DNS records is out of scope of this document. However, guidance can be found here:  
<https://developer.okta.com/docs/guides/custom-url-domain/main/>.
- The guidance may need to be adapted to the specific domain setup.
- Contact your DNS administrator to coordinate all actions.

4. DNS details will be provided on the next screen. Modify the DNS records with these values.

**Update your DNS**

To serve traffic over your domain, you need to add DNS records to point to Okta.  
Sign in to your registrar or DNS provider and add these entries.  
It may take a few minutes for the DNS changes to be available globally. You can check the availability of your records with a DNS lookup tool.  
After the DNS records are updated, return here for Okta to verify them.

[Docs](#)

Type	Host	Value
TXT	_acme-challenge.stig[redacted].com	[redacted]
CNAME	stig[redacted].com	[redacted].customdomains.oktapreview.com

Save for later **Next**

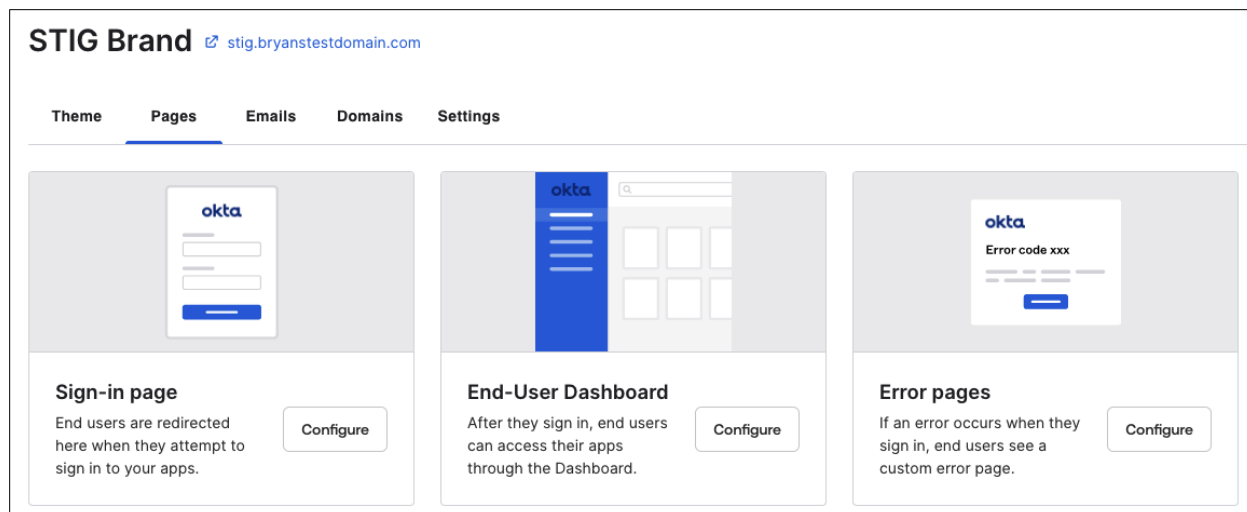
5. After the DNS is set in the register, click **Next**. Verify the values. If an error is returned, you may need to wait for the new DNS records to propagate.
6. Validate your own TLS certificate by following the instructions here:  
<https://developer.okta.com/docs/guides/custom-url-domain/main/#use-your-own-tls-certificate>
7. When done, click **Finish**.

### 3.3 Modifying the Sign-In Page

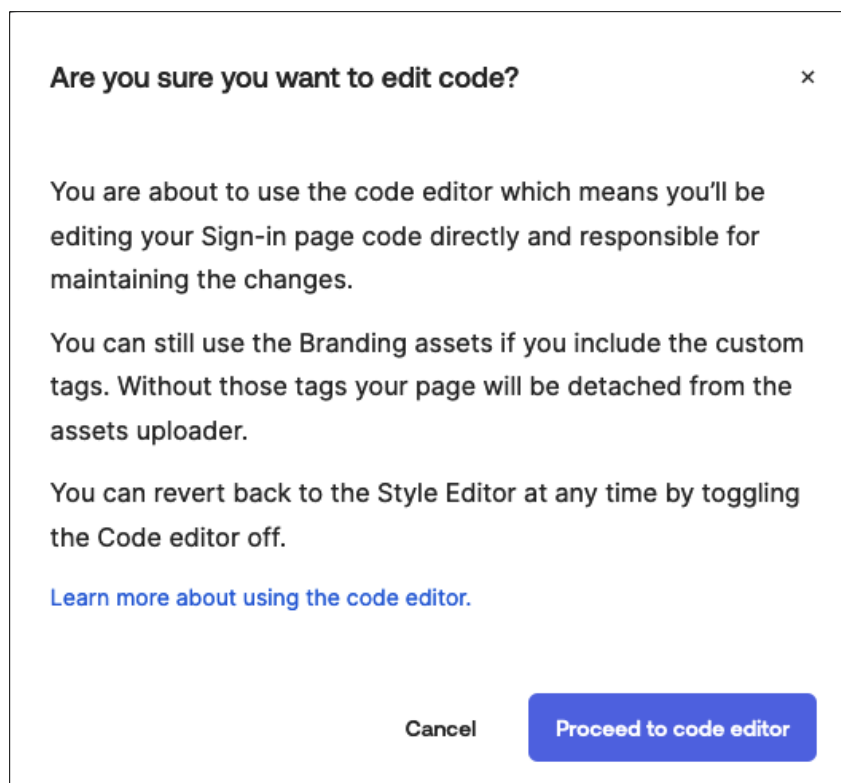
1. While in the Brand created earlier (Admin >> Customizations >> Brands >> the brand created in the Create a Brand section of this document), click **Pages**.



2. In the **Sign-in page** section, click **Configure**.



3. Toggle the switch for **Code editor**. When prompted, click **Proceed to Code Editor**.



- The screen will show the code for the sign-in page. You will be modifying the HTML in the `<head>` section of the code.



```

1 <!DOCTYPE html PUBLIC "-//W3C//DTD HTML 4.01//EN" "http://www.w3.org/TR/html4/strict.dtd">
2 <html>
3 <head>
4   <meta http-equiv="Content-Type" content="text/html; charset=UTF-8">
5   <meta name="viewport" content="width=device-width, initial-scale=1.0" />
6   <meta name="robots" content="noindex,nofollow" />
7   <!-- Styles generated from theme -->
8   <link href="{{themedStylesUrl}}" rel="stylesheet" type="text/css">
9   <!-- Favicon from theme -->
10  <link rel="shortcut icon" href="{{faviconUrl}}" type="image/x-icon"/>
11
12  <title>{{pageTitle}}</title>
13  {{SignInWidgetResources}}
14
15  <style nonce="{{nonceValue}}">
16    #login-bg-image-id {
17      background-image: {{bgImageUrl}}
18    }
19  </style>
20 </head>

```

- Click **Edit** in the upper-right corner to edit the code.
- Add in the following code, enclosed in `<script>` `</script>` tags (opening and closing):

```

alert("You are accessing a U.S. Government (USG) Information System (IS) that
is provided for USG-authorized use only. By using this IS (which includes any
device attached to this IS), you consent to the following conditions: -The USG
routinely intercepts and monitors communications on this IS for purposes
including, but not limited to, penetration testing, COMSEC monitoring, network
operations and defense, personnel misconduct (PM), law enforcement (LE), and
counterintelligence (CI) investigations. -At any time, the USG may inspect and
seize data stored on this IS. -Communications using, or data stored on, this IS
are not private, are subject to routine monitoring, interception, and search,
and may be disclosed or used for any USG-authorized purpose. -This IS includes
security measures (e.g., authentication and access controls) to protect USG
interests--not for your personal benefit or privacy. -Notwithstanding the
above, using this IS does not constitute consent to PM, LE or CI investigative
searching or monitoring of the content of privileged communications, or work
product, related to personal representation or services by attorneys,
psychotherapists, or clergy, and their assistants. Such communications and work
product are private and confidential. See User Agreement for details.")

```

7. The code will now look like this:

```

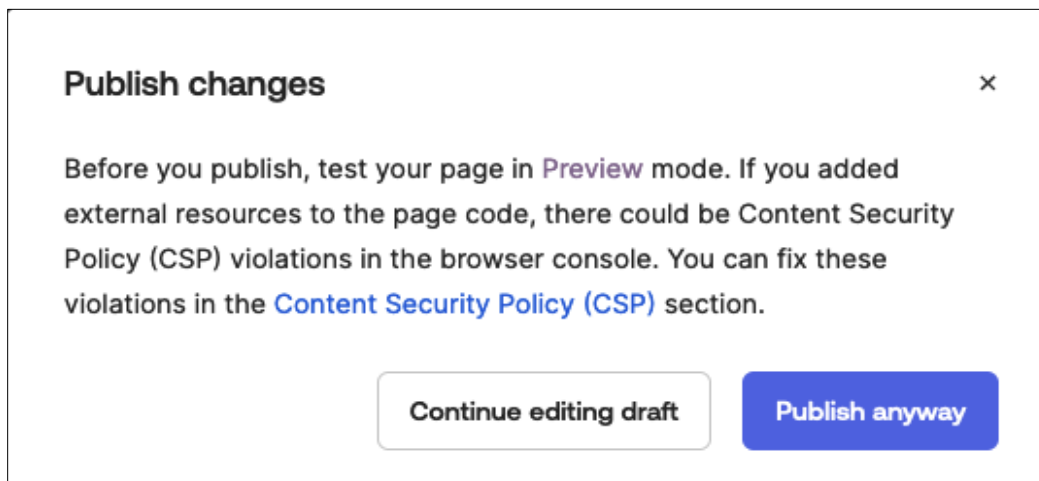
5 <meta name="viewport" content="width=device-width, initial-scale=1.0" />
6 <meta name="robots" content="noindex,nofollow" />
7 <!-- Styles generated from theme -->
8 <link href="{{themedStylesUrl}}" rel="stylesheet" type="text/css">
9 <!-- Favicon from theme -->
10 <link rel="shortcut icon" href="{{faviconUrl}}" type="image/x-icon"/>
11
12 <title>{{pageTitle}}</title>
13 <!-- Sign-in widget resources -->
14
15 <style nonce="{{nonceValue}}">
16   #login-bg-image-id {
17     background-image: {{bgImageUrl}}
18   }
19 </style>
20 <script>alert("You are accessing a U.S. Government (USG) Information System (IS) that is provided for USG-authorized use only. By
21 </head>
22 <body>
23 <div id="login-bg-image-id" class="login-bg-image the-background"></div>

```

8. Click **Save to draft** in the upper-right corner.
9. Click **Preview** at the top of the page to preview the new sign-in page before publishing.



10. A new page will pop up and display the banner. Click **OK** on the pop-up to load the sign-in page. Ignore the note about the CSP policy.
11. Click on **Publish**. When the CSP warning pops up, click **Publish anyway**.



12. Navigate to the sign-in page in a private/logged-out browser to view the pop-up.